jamk.fi

Palautumissuunnittelu ja automatisoitu Active Directory -palautustestaus

Mika Tuoriniemi

Opinnäytetyö
Helmikuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Tuoriniemi, Mika	Opinnäytetyö, AMK	Helmikuu 2020
	Sivumäärä 55	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Palautumissuunnittelu ja automatisoitu Active Directory -palautustestaus

Tutkinto-ohjelma
Insinööri (AMK), tieto- ja viestintätekniikka

Työn ohjaaja(t)
Sampo Kotikoski, Pasi Heikkinen

Toimeksiantaja
Telia Inmics-Nebula

Tiivistelmä

Telia Inmics-Nebula on Telia Companyn B2B perheeseen kuuluva IT-palveluntarjoaja, joka tarjoaa asiantuntijapalveluita monelle eri osa-alueelle, kuten pilvipalveluihin, konesalipalveluihin ja laitehallintaan.

Opinnäytetyön tarkoituksena oli tutkia palautumissuunnittelua yleisellä tasolla. Tavoitteena oli saavuttaa lähtökohta organisaation IT-infrastruktuurin palautumissuunnittelun rakentamiselle. Tutkimisen lisäksi tutustuttiin teknisellä toteutuksella tarkemmin yhteen palautumissuunnittelun osa-alueeseen, palautustestaukseen.

Palautustestaus toteutettiin itse rakennetulle virtuaaliselle Active Directory -palvelulle hyödyntäen Veeam Backup & Replication -ohjelmistoa sekä sen Surebackup -toiminnallisuutta.

Testauksen tavoitteena oli demonstroida automatisoitua palautustestausta ja sen hyötyjä itse varmuuskopioiden tueksi.

Työn tuloksena saatiin selvitettyä palautumissuunnittelun hyötyjä, sen kriittisimmät osa-alueet, mitä ja kuinka ne tulee huomioida ja kuinka voidaan lähteä rakentamaan organisaation IT-infrastruktuurin palautumissuunnittelua. Samalla tuotiin esille automatisoidun palautustestauksen hyötyjä. Merkittävin hyöty automatisoidussa palautustestauksessa saadaan siitä, että suurien kokonaisuuksien testaaminen voidaan suorittaa automatisoidusti suoraan varmuuskopioinnin jälkeen. Tällä saadaan samalla varmistettua varmuuskopiointien toimivuus.

Avainsanat (asiasanat)
Palautumissuunnittelu, palautustestaus

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Tuoriniemi, Mika	Bachelor's thesis	February 2020
		Language of publication: Finnish
	Number of pages: 55	Permission for web publication: x

Title of publication

Disaster Recovery Planning and automated Active Directory recovery verification

Degree programme

Bachelor of Engineering, Information Technology

Supervisor(s)

Sampo Kotikoski, Pasi Heikkinen

Assigned by

Telia Inmics-Nebula

Abstract

Telia Inmics-Nebula is an IT -service provider that belongs to Telia Company's B2B family. Telia Inmics-Nebula offers specialist services in multiple different areas of IT, for example in cloud services, datacenter services and device management.

The purpose of this assignment was to study disaster recovery planning on a general level as well as look deeper into one part of disaster recovery, namely recovery verification.

Disaster recovery was studied to gain a general overview of what is needed in the planning phase and to provide all the necessary information to a successful disaster recovery plan.

Recovery verification was carried out on a self-hosted virtualized Active Directory service using Veeam Backup & Replication and its Surebackup function. The purpose of this testing was to demonstrate the benefits of Recovery Verification to support backups.

As a result, the benefits and the, most critical parts were documented as well as, what needs to be taken into consideration and how to start building a disaster recovery plan for an organization's IT-infrastructure. The benefits of an automated recovery test were also demonstrated and, why it is necessary as well as ways how it can make an organization more confident in its ability to recover from a disaster.

Keywords/tags (subjects)

Disaster recovery, recovery verification

Miscellaneous (Confidential information)

Sisältö

Kuviot

Lyhenteet

AAIP	Application Aware Image Processing
AD DS	Active Directory Domain Services
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CRC	Cyclic Redundancy Check
DC	Domain Controller
DNS	Domain Name System
DRP	Disaster Recovery Plan
HDD	Hard Disk Drive
IAM	Identity and Access Management
IMP	Incident Management Plan
ISMS	Information Security Management System
LAN	Local Area Network
OU	Organizational Unit
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
vCPU	Virtual Central Processing Unit
VLAN	Virtual Local Area Network
VSS	Volume Shadow Copy
WAN	Wide Area Network

1 Johdanto

1.1 Toimeksiantaja

Telia Inmics-Nebula on Telian B2B-perheeseen kuuluva yritys, joka omaa laajaa asiantuntemusta mm. pilvipalveluista, edistyksellisten ICT-ympäristöjen sekä loppukäyttäjäpalveluiden tuottamisesta. (Telia Inmics-Nebula 2019.)

Yhtenä tuotteena Telia Inmics-Nebula tarjoaa asiakkailleen varmistuspalveluita, joihin sisältyy asiakkaan virtualisoidun tai fyysisen palvelinympäristön sekä työasemien varmuuskopioinnin suunnittelu, käyttöönotto sekä ylläpitäminen.

1.2 Tutkimusmenetelmä ja -kysymykset

Opinnäytetyöllä haluttiin vastata lähtökohtaisesti seuraaviin kysymyksiin:

1) Onko mahdollista toteuttaa automaattinen palautustestaus osana palautumissuunnittelua?
2) Kuinka palautustestaus palvelee palautumissuunnittelua ja jatkuvuussuunnittelua?
3) Kuinka palautumissuunnittelua voidaan toteuttaa?
4) Mitä palautumissuunnittelu antaa yritykselle?

Tutkimusmenetelmänä käytettiin laadullista tutkimusta. Tutkimuksessa hyödynnettiin aikaisempia tutkimuksia palautumissuunnittelusta sekä palautustestauksesta. Aluksi tutkittiin palautumissuunnitelmaa yleisellä tasolla, minkä jälkeen työn soveltavassa vaiheessa keskityttiin palautumissuunnitelman yhteen osa-alueeseen: palautustestaukseen.

1.3 Tarve ja tavoitteet

Opinnäytetyön tarkoituksena oli tutkia palautumissuunnittelua Telia Inmics-Nebula Oy:lle. Palautumissuunnittelua on tutkittu ja tehty paljon, joten tämän työn tarkoituksena oli kasvattaa lukijan ymmärrystä palautumissuunnittelusta sekä antaa lähtökohta palautumissuunnittelun tekemiselle.

Miksi palautumissuunnittelu on niin tärkeää yrityksen toiminnan kannalta?

Maailma on siirtymässä entistä enemmän digitalisoituneempaan suuntaan ja palveluiden sekä datan saatavuuden merkitys kasvaa. Jokainen yritys on jollain tavalla riippuvainen omasta IT-infrastruktuuristaan eikä mikään yritys ole täysin turvassa katastrofeilta. Erilaisia riskitekijöitä voivat olla esim. tulipalot tai sähkökatkokset. Mitä tapahtuu, kun laaja sähkökatkos katkaisee yrityksesi tarjoamat palvelut 24 tunnin ajaksi? Kuinka paljon tämä maksaa yrityksellesi? Nykypäivänä palveluiden toiminnan jatkuvuus on elintärkeää, pienetkin katkokset voivat aiheuttaa suuria tappioita yrityksen liiketoiminnalle.

2 Jatkuvuussuunnittelu

Jatkuvuussuunnitelma (engl. Business continuity plan, BCP) on prosessi, minkä avulla pyritään luomaan ehkäisy- sekä palautumisjärjestelmä, jolla turvataan yrityksen palveluiden jatkuvuutta. Jatkuvuussuunnitelman tarkoituksena on turvata yrityksen avainhenkilöt sekä muu tärkeä omaisuus katastrofin sattuessa. Jatkuvuussuunnitelma on osana määrittämässä kaikkia yrityksen palveluita uhkaavia riskitekijöitä tehden siitä tärkeän osan yrityksen riskienhallintastrategiaa. Jatkuvuussuunnitelma on tarkoitettu auttamaan yritystä palauttamaan normaali toiminta esimerkiksi tulipalon sattuessa. Se kattaa paljon suuremman osan yrityksen toiminnasta kuin palautumissuunnitelma, joka käsittelee yrityksen IT-järjestelmien palautumista kriisin jälkeen. (Kenton 2019.)

Jatkuvuussuunnittelun osa-alueet

Jatkuvuussuunnitelma voidaan luoda yritykselle jonkin yksittäisen prosessin turvaamiseksi tai sen voi kohdistaa kaikkiin liiketoiminnan kannalta kriittisiin prosesseihin. Kuten aikaisemmin mainittiin, jatkuvuussuunnitelma on suurempi kokonaisuus, jossa palautumissuunnittelu on vain yksi sen osa-alueista. Muut jatkuvuussuunnitelman osat ovat

1. Business Resumption Plan
2. Occupant Emergency Plan
3. Incident Management Plan
4. Continuity of Operations Plan
5. Disaster Recovery Plan.

Näistä viidestä vain kaksi keskittyy varsinaisesti IT-järjestelmiin: tietoturvapoikkeamien hallintasuunnitelma (engl. Incident Management Plan, IMP) sekä palautumissuunnitelma. (Bahan 2003.)

IMP määrittää rakenteen ja toimintatavat, joilla käsitellään kyberhyökkäyksiä yrityksen IT-järjestelmiä vastaan eikä yleensä johda palautumissuunnitelman käyttöönottoon. (Mt.)

3 Palautumissuunnittelu

3.1 Yleistä

Palautumissuunnitelma (engl. Disaster recovery plan, DRP) konseptina kehiteltiin 1970 luvun lopulla, kun tietokonekeskusten ylläpitäjät alkoivat ymmärtämään organisaatioiden olevan riippuvaisia tietokonejärjestelmistään. Näihin aikoihin suurin osa järjestelmistä oli suurtietokoneita, jotka pystyivät olemaan alhaalla useita päiviä ennen suuren vahingon aiheutumista. (Disaster Recovery n.d.)

Kun tietokonejärjestelmistä alkoi kehittyä kriittisempiä järjestelmiä organisaation toiminnan kannalta, myös niiden toiminnan varmistamisen ja nopean toiminnan palauttamisen tarve kasvoi. (Mt.)

Tiedon saatavuus on yksi tietoturvan kulmakivistä. Saatavuudella viitataan siihen, että verkot, järjestelmät ja sovellukset ovat *päällä ja saavutettavissa*. Monet asiat voivat vaarantaa saatavuutta, mukaan lukien komponenttien tai sovelluksien hajoamiset, luonnonkatastrofit ja ihmisten tekemät virheet. (Walkowski 2019.)

Nykypäivänä erilaiset haittaohjelmat, kuten kiristyshaittaohjelmat, uhkaavat tiedon saatavuutta. Palautumissuunnittelu ja varmistukset ovat yksi tapa, jolla tätä riskiä voidaan pienentää.

3.2 ISO/IEC 27000 -standardit

ISO/IEC 27000 -standardiperhe kuvaa tietoturvallisuuden hallintajärjestelmiä. Tietoturvallisuuden hallintajärjestelmiä käsitteleviä malleja voidaan noudattaa hallintajärjestelmän luonnissa sekä käytössä. Näiden standardien käytön on tarkoitus avustaa kaikentyyppisiä ja -kokoisia organisaatioita toteuttamaan ja käyttämään tietoturvallisuuden hallintajärjestelmää. (SFS-EN ISO/IEC 27000:2017, 5.)

ISO/IEC 27000 -standardiperhe on sarja toisiaan tukevia tietoturvallisuuden standardeja, jotka yhdessä toimittavat globaalisti tunnetun viitekehyksen parhaita käytäntöjä varten tietoturvallisuuden hallinnassa (ISO 27000 Series of Standards n.d.).

ISO 27001 (Tietoturvallisuuden hallintajärjestelmät)

ISO 27001 -standardissa määritellään vaatimukset, jotka koskevat tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista organisaation toimintaympäristössä (SFS-EN ISO/IEC 27001:2017, 5).

Tietoturvallisuuden hallintajärjestelmä (engl. Information Security Management System, ISMS) on tietoturvallisuuden hallintajärjestelmä, joka on määrämuotoinen tapa kerätä yhteen kaikki tietoturvaan liittyvät aktiviteetit ja toimia hallitusti. Monissa yrityksissä tietoturvanäkökohtia on yleensä jollain tavalla huomioitu käytännön tasolla, mutta niiden tehokkuutta ei kyetä mittaamaan asianmukaisesti. (Tuominen 2019.)

Tietoturvallisuuden hallintajärjestelmä koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä resursseista ja toiminnoista, joita organisaatio hallinnoi kootusti suojatakseen tieto-omaisuuttaan. Tietoturvallisuuden hallintajärjestelmä perustuu riskien arviointiin ja organisaation riskien hyväksyntätasoihin, jotka on suunniteltu riskien tahokasta käsittelyä ja hallintaa varten. (SFS-EN ISO/IEC 27000:2017, 19.)

ISO 27002 (Tietoturvallisuuden hallintakeinojen menettelyohjeet)

ISO 27002 on lisästandardi, joka sisältää hallintakeinoja tietoturvallisuuden kehittämiseen. Kontrollit löytyvät myös ISO 27001 -standardin liitteestä A, mutta ISO 27002 sisältää paljon syvällisemmän katsauksen. Selittäen, kuinka kontrollit toimivat, mikä niiden tavoite on ja kuinka niitä voidaan toteuttaa. (Irwin 2019.)

> *Tässä standardissa esitetään organisaation tietoturvastandardeja ja tietoturvallisuuden hallintakäytänteitä koskevaa ohjeistusta, johon sisältyy hallintakeinojen valinta, toteuttaminen ja hallinta ottaen huomioon organisaation tietoturvallisuuden riskiympäristöt. (SFS-EN ISO/IEC 27002:2017, 8.)*

ISO 27005 (Tietoturvariskien hallinta)

ISO 27005 on kansainvälinen standardi, joka käsittelee riskien arvioinnin toteutusta ISO 27001:n määriteltyjen vaatimusten mukaisesti. Tämä standardi korostaa systemaattista lähestymistapaa rakentaa ja ylläpitää ISRM (Information Security Risk Management) -prosessia ja muistuttaa, että riskienhallinnan tulee olla jatkuvaa, jotta voidaan varmistaa jatkuva toiminnallisuus. (Veltsos 2018.)

3.3 Riskienhallinta ja riskianalyysi

Riskienhallinta

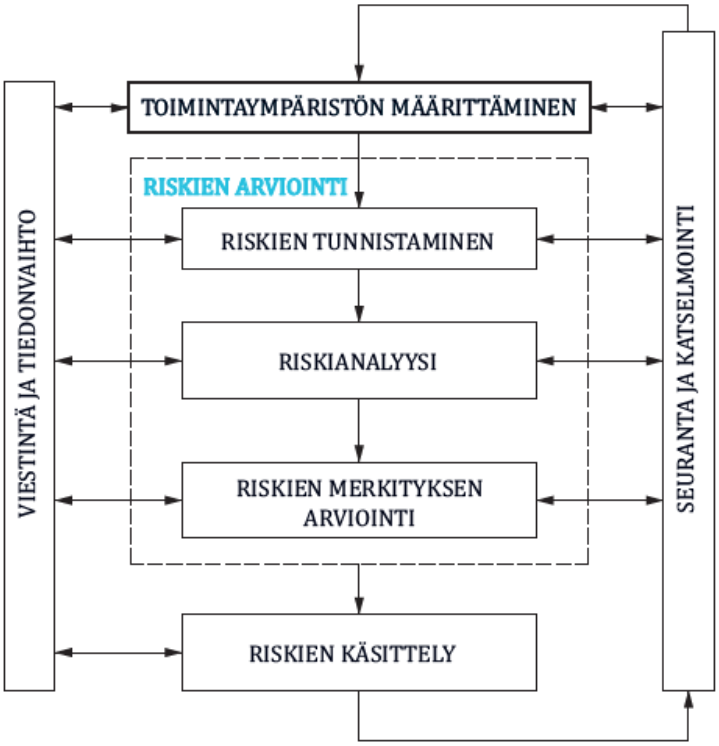
Organisaation toimintaan liittyy aina riskejä, nämä riskit yleensä uhkaavat tavoitteiden saavuttamista. Merkittävimpiä kohteita riskeillä voivat olla esimerkiksi toiminnan jatkuvuus tai sen häiriöttömyys. Riskien tunnistaminen, analysointi ja niiden vaikutusten arviointi ovat osa hyvän riskianalyysin osa-alueita. (Riskianalyysit n.d.)

Riskienhallintaa voidaan tehdä monella eri keinoilla. Ensisijaisesti täytyy pyrkiä estämään vahingon syntyminen tai vähentämään riskin aiheuttamia seurauksia. Tarve toimenpiteille muodostuu kuitenkin siitä, kuinka vakava riski on. Mitä suurempi riski, sitä suurempi tarve on pienentää sen mahdollisuutta ja sen vaikutuksia. (Riskienhallintaprosessi n.d.)

Riskienhallinnalla on selkeät vaiheet, ensin on tunnistettava ja arvioitava, minkä jälkeen suunnitellaan riskien hallitsemiseksi tarvittavat toimenpiteet. Viimeisessä vaiheessa tilannetta ja toimenpiteiden vaikutusta valvotaan sekä raportoidaan johtohenkilöstölle tilanteesta. (Mt.)

Riskienhallinnalla haetaan tukea strategian toteutumista ja saavuttamista varten. Yrityksen riskienhallintaprosessin tavoitteena on varmistaa, että riskienhallinnalla on yhtenäinen toimintamalli ja että johto saa riittävästi tietoa riskeistä päätöksenteon tueksi.

Alla olevassa kuviossa (ks. Kuvio 1) on esitetty riskienhallintaprosessi ISO 27005 -standardin määrittelemänä.



Kuvio 1. Riskienhallintaprosessi (SFS-EN ISO/IEC 27005:2018, 8)

Periaatteena on ennaltaehkäisevästi huomioida kaikki riskit. Riskienhallinta perustuu riskien tunnistamiseen, arviointiin ja raportointiin. Riskienhallinta on kiinteä osa päivittäistä toimintaa ja vuosittaista strategista suunnittelua.

Riskianalyysi

Riskianalyysi on prosessi, jossa tunnistetaan ja analysoidaan potentiaaliset ongelmat, jotka voivat vaikuttaa negatiivisesti yrityksen keskeisiin liiketoiminnallisiin aloitteisiin ja projekteihin. Riskianalyysillä haetaan helpotusta riskien välttämiseen ja vähentämiseen. (Rouse 2018d.)

Riskien tunnistamisen jälkeen, ne analysoidaan laadullisen ja määrällisen vaikutuksen määrittämistä varten, jotta riskienhallintaa varten voidaan tehdä tarvittavat jatkotoimenpiteet (Lavanya & Malarvizhi 2008).

Seuraavia linjauksia voidaan käyttää apuna riskianalyysissä:

1) Riskin todennäköisyys
   - Korkea – (80% ≤ x ≤ 100%)
   - Keskitaso-korkea – (60% ≤ x ≤ 80%)
   - Keskitaso-matala – (30% ≤ x ≤ 60%)
   - Matala – (0% ≤ x ≤ 30%)

2) Riskin vaikutukset
   - Korkea – Katastrofinen (A – 100)
   - Keskitaso – Kriittinen (B – 50)
   - Matala – Marginaalinen (C – 10) (Mt.)

Riskien todennäköisyyksien ja vaikutusten määritysten jälkeen voidaan koota seuraavanlainen matriisi riskianalyysiä varten. (ks. Kuvio 2.)

		Probability			
		1 = high (80% ≤ x ≤ 100%)	2 = medium high (60% ≤ x < 80%)	3 = medium low (30% ≤ x < 60%)	4 = low (0% < x < 30%)
Impact	A=high (Rating 100)	(Exposure – Very High) (Score 100)	(Exposure – Very High) (Score 80)	(Exposure – High) (Score 60)	(Exposure – Moderate) (Score 30)
	B=medium (Rating 50)	(Exposure – High) (Score 50)	(Exposure – Moderate) (Score 40)	(Exposure – Moderate) (Score 30)	(Exposure – Low) (Score 15)
	C=low (Rating 10)	(Exposure – Low) (Score 10)	(Exposure – Low) (Score 8)	(Exposure – Low) (Score 6)	(Exposure – Low) (Score 3)

Kuvio 2. Riskianalyysi matriisi (Mt.)

Väreillä kuvastetaan riskien vastatoimien suunnittelun kiireellisyyttä ja määritellään raportointitasot (Mt.).

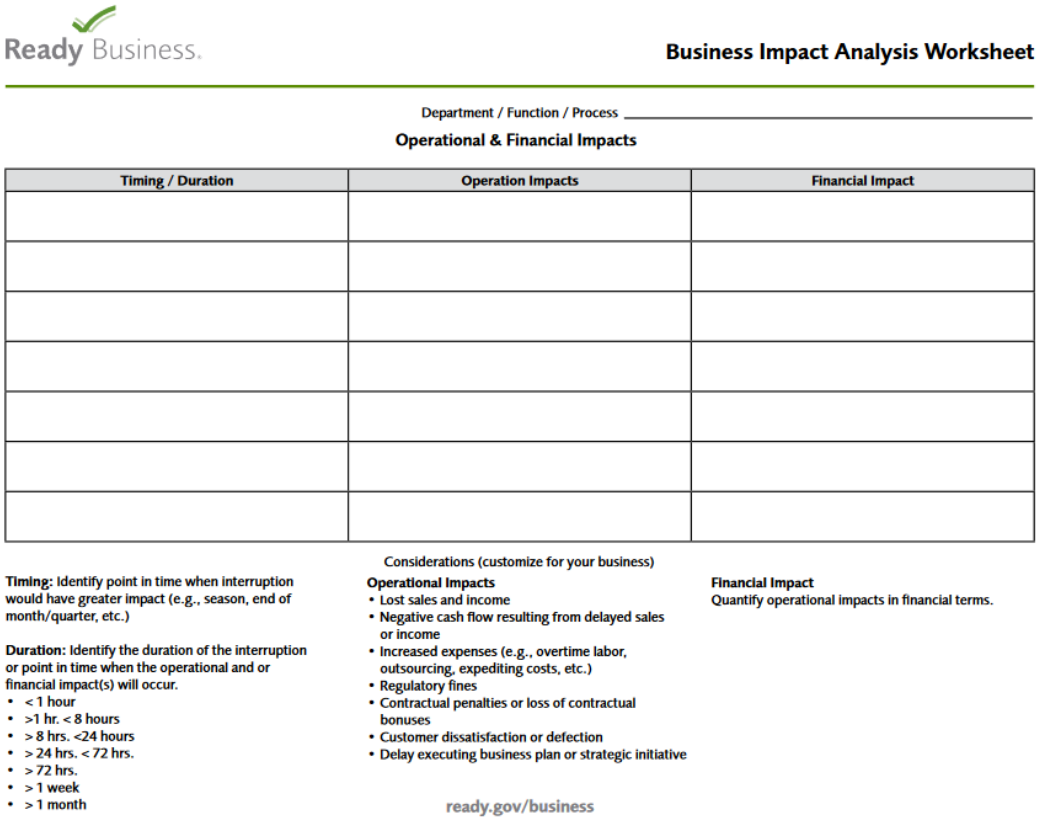
3.4 Liiketoiminnalle aiheutuvat vaikutukset

Katastrofeista aiheutuvia vaikutuksia liiketoiminnalle analysoidaan ns. Business Impact Analysis (BIA) avulla. BIA on prosessi, jolla pyritään ymmärtämään ja analysoimaan yrityksen liiketoimintaa ja liiketoiminnan katkeamisen vaikutuksia. Jotkin liiketoiminnan kannalta kriittiset toiminnot eivät voi olla alhaalla montaakaan tuntia, kun jotkin taas kestävät katkoksia päiviä tai jopa viikkoja riippuen tilanteesta. BIA yleensä tarkoittaa kattavaa tutkimusta tiedon keräämiselle, ennen kuin määritellään BIA -malli tai suunnittelutoimenpiteet sekä parannuskeinot katastrofeja varten. (Salleh 2013.)

BIA:n avulla pitäisi pystyä tunnistamaan toiminnalliset sekä taloudelliset vaikutukset liiketoiminnan keskeytymisen aiheutuessa. Vaikutuksia arvioitaessa tulisi ottaa huomioon ainakin seuraavat aihealueet:

- Menetetyt myynnit ja tulot
- Myöhästyneet myynnit tai tulot
- Suuremmat kulut (ylityömaksut, palveluiden ulkoistaminen)
- Asiakastyytymättömyys
- Sopimusrikkomukset (esim. Palvelutaosopimukset). (Business Impact Analysis n.d.)

Federal Emergency Management Agency (FEMA) tarjoaa BIA:n tekemiseen valmiin pohjan, jossa määritellään mm. mihin aikaan (vuodenaika, kuun loppu/alku, kvartaali) katkoksella on suurimmat vaikutukset, katkoksen kesto (tunteja, päiviä, viikkoja), toiminnalliset vaikutukset (menetetyt myynnit ja tulot, suuremmat kulut) ja taloudellinen vaikutus. (Ks. Kuvio 3.)



Ready Business.

Business Impact Analysis Worksheet

Department / Function / Process _____

Operational & Financial Impacts

Timing / Duration	Operation Impacts	Financial Impact

Considerations (customize for your business)

Timing: Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter, etc.)

Duration: Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur.

- < 1 hour
- >1 hr. < 8 hours
- > 8 hrs. <24 hours
- > 24 hrs. < 72 hrs.
- > 72 hrs.
- > 1 week
- > 1 month

Operational Impacts

- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative

Financial Impact
Quantify operational impacts in financial terms.

ready.gov/business

Kuvio 3. BIA Worksheet (Business Impact Analysis Worksheet 2014)

3.5 Henkilöstö ja kommunikointi

Palautumissuunnittelussa oleellista on kommunikoida tehokkaasti muille osapuolille. Tällä turvataan se, että suunnitelma saadaan toteutettua sen määrittämissä aikamääreissä onnistuneesti. Kommunikointia helpottaa, kun luodaan lista tarvittavista yhteyshenkilöistä. Listassa tulisi olla yhteystiedot, josta henkilöt saadaan tavoitettua. Henkilöillä tulee olla myös varahenkilöt, sillä tiettyä osa-aluetta ei voida jättää yhden ihmisen varaan, jos sattuu käymään niin, että tehtävään määritetty henkilö on saavuttamattomissa.

Palautumissuunnittelussa määritelty tiimi on ryhmä henkilöitä, jotka kehittävät, dokumentoivat ja toteuttavat prosessit organisaation datan, palveluiden jatkuvuuden sekä IT-infrastruktuurin palauttamisen kannalta katastrofin sattuessa. Tiimin roolit

täytyy määrittää tarkasti, jotta kaikki ovat varmoja siitä, mistä vastaavat oikean tilanteen tullen.

Tiimi rakennetaan pääsääntöisesti organisaation omasta henkilöstöstä, mutta huomioon tulee ottaa myös mahdolliset sovellustoimittajat, jotka voivat toimia tukihenkilöinä tietyn sovelluksen toimintaan palauttamisessa.

3.6 Varmuuskopiointi

3.6.1 Yleistä

Varmuuskopiointi viittaa tiedon kopioimiseen toiseen sijaintiin alkuperäisen tiedon katoamisen tai hajoamisen varalta, josta se voidaan palauttaa takaisin. Varmuuskopiointi on yksi palautussuunnittelun keskeisimmistä osista, jonka tavoitteena on suojautua tiedon menettämiseltä. (Rouse 2018b.)

Tietoturvallisuutta tukeva CIA-malli muodostuu kolmesta eri kohdasta: luotettavuudesta, eheydestä ja saatavuudesta. Varmuuskopiointi on yksi keskeisimmistä tavoista parantaa tiedon saatavuutta, täten ollen kytköksissä jokaisen organisaation tietoturvalliseen toimintaan.

ISO 27002 -standardin mukaisesti tiedoista, ohjelmistoista ja järjestelmistä olisi otettava säännöllisesti varmuuskopiot, jotka olisi testattava sovittujen varmuuskopiointiperiaatteiden mukaisesti. Varmuuskopioinnin toteuttamiseen ISO 27002 -standardi tarjoaa toteuttamisohjeita, joita voidaan soveltaa oman varmuuskopiointipolitiikan luomiseen. SFS-EN ISO/IEC 27002:2017, 50-51.)

Varmuuskopiointisuunnitelman suunnittelussa tulisi ottaa huomioon seuraavat ohjeet:

- Varmuuskopioista ja dokumentoiduista palautusmenettelyistä olisi tuotettava tarkat ja täydelliset tallenteet

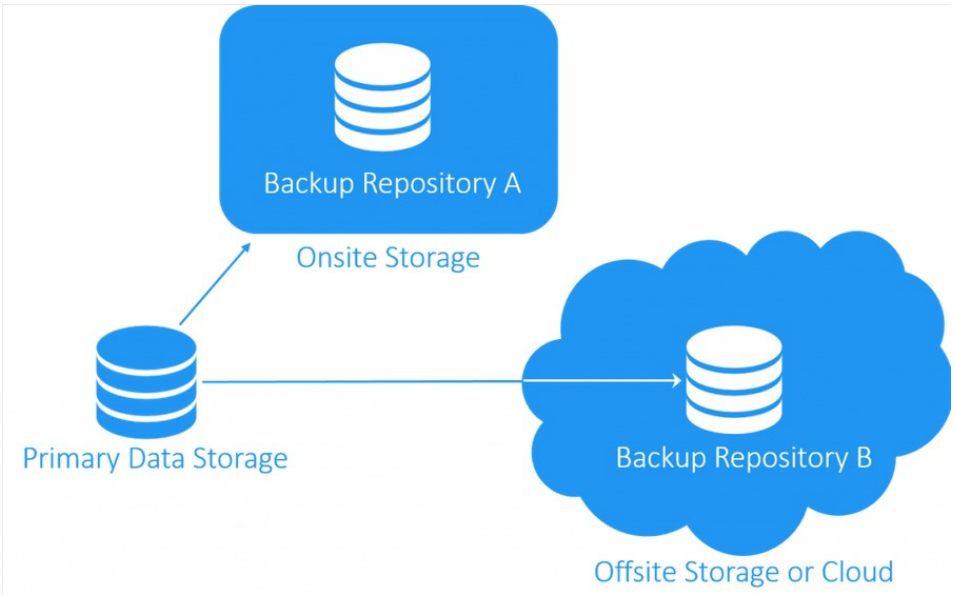
- Varmuuskopioinnin laajuuden (esim. täydellinen vai osittainen kopio) ja varmuuskopioinnin suoritusvälin olisi kuvastettava organisaation liiketoimintavaatimuksia, kyseisen tiedon turvallisuusvaatimuksia ja tiedon kriittisyyttä organisaation toiminnan jatkumisen kannalta
- Varmuuskopiot olisi varastoitava erillä olevaan paikkaan, joka on riittävän kaukana välttyäkseen pääkäyttöpaikalla tapahtuvan katastrofin aiheuttamalta vahingolta
- Varmuuskopioiden tiedot olisi suojattava sekä fyysisesti että ympäristöuhilta pääkäyttöpaikalla noudatettavan vaatimustason mukaisesti
- Varmuuskopioiden tietovälineet olisi testattava säännöllisesti, jotta voidaan varmistua siitä, että hätätilanteessa niihin voidaan luottaa. Tämä olisi yhdistettävä palautumismenettelyjen testaukseen ja tarkistettava vaaditun palautusajan suhteen. Varmuuskopioidun tiedon palautuskyvyn testaus olisi suoritettava määritellyllä testivälineellä, mutta ylikirjoittamatta alkuperäistä tietoa, sillä varmuuskopiointi- tai palautusprosessin epäonnistuminen voisi aiheuttaa korjaamatonta vahinkoa tai hävikkiä
- Jos luottamuksellisuus on tärkeää, varmuuskopiot olisi suojattava salauksella (Mts. 51.)

Varmuuskopiointi voidaan suorittaa tiedostotasolla tai imagetasolla. Tiedostotason varmuuskopiointi mahdollistaa yksittäisten tiedostojen ja kansioiden varmuuskopioinnin tietokoneeltasi toiseen sijaintiin. Tiedostotason varmuuskopiointi on hyvä ratkaisu, jos halutaan pitää vain tietyt tiedostot tallessa, kuten PowerPoint esitykset. Todellisen katastrofin sattuessa tietokoneen toimintakuntoon palauttaminen voi olla kuitenkin työläs prosessi.

Imagetason varmuuskopio on paljon kattavampi vaihtoehto varmuuskopioinnille. Imagetason varmuuskopioinnissa koko käyttöjärjestelmästä ja sen sisältämästä tiedosta otetaan tilannevedos (engl. Snapshot). Tilannevedos sisältää kaiken kiintolevyllä olevan datan käyttöjärjestelmästä lähtien. Imagetason varmuuskopiosta vaatii säilytystä varten enemmän kapasiteettia ja varmuuskopioinnin suorittamisessa yleensä kestää kauemmin, mutta sen hyödyt ovat suuret verrattuna tavalliseen tiedostotason varmuuskopiointiin. Imagetason varmuuskopiosta voidaan palauttaa myös yksittäisiä tiedostoja, jos koko tietokoneen palauttaminen ei ole tarpeellista.

3-2-1 Sääntö

Varmuuskopioinnissa 3-2-1 sääntö on helposti muistettava suositus, minkä avulla voidaan olla varmoja, että tiedot ovat tallessa melkein missäpä tahansa katastrofitilanteessa. Säännön mukaan tulisi säilyttää **kolme** kopiota tiedoista **kahdella** eri medialla (kiintolevy, varmistusnauha), joista **yksi** on toisessa sijainnissa. (Ks. Kuvio 4.)

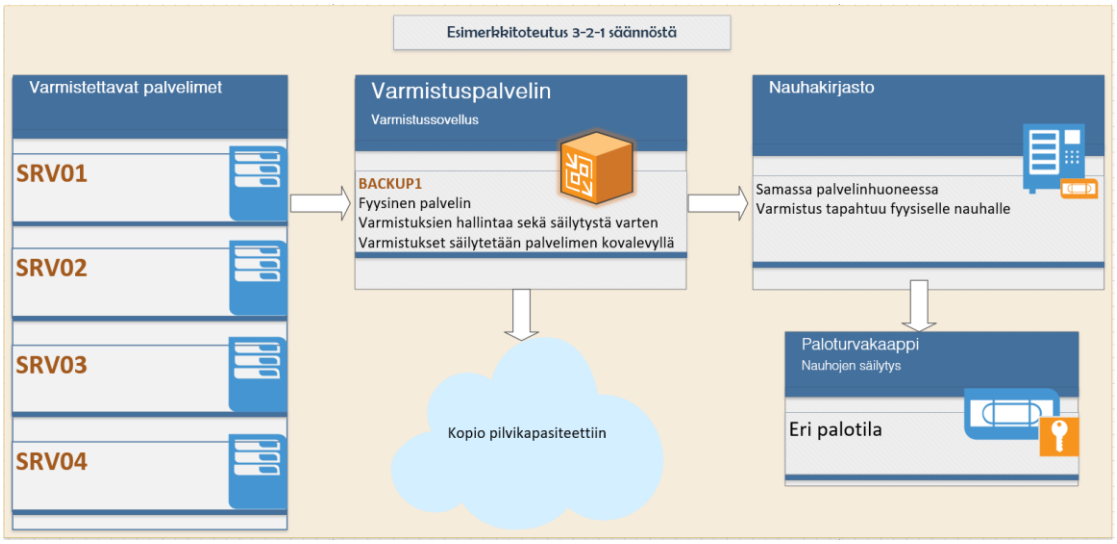


Kuvio 4. 3-2-1 sääntö (Mayer 2017)

Sääntö antaa hyvän pohjan lähteä rakentamaan varmuuskopiointisuunnitelmaa, ja suunnittelussa tulee ottaa huomioon hyvin paljon eri asioita kuten kriittiset sijainnit, varmuuskopiotyypit, säilytysmedia, ajastukset, automaatio, kryptaus ja testaus eri skenaarioiden avulla (Mayer 2017).

Yksi esimerkki 3-2-1 säännön täyttämästä varmuuskopiointiympäristöstä (ks. Kuvio 5) voisi olla seuraavanlainen:

- Varmistukset suoritetaan varmistuspalvelimen paikalliselle levylle päivittäin
- Varmistukset kopioidaan pilvikapasiteettiin
- Varmistukset suoritetaan myös fyysiselle varmistusnauhalle levyvarmistuksen jälkeen
- Nauhavarmistukset säilytetään erillisessä paloturvakaapissa, eri palotilassa.



Kuvio 5. Esimerkkitoteutus 3-2-1 -säännöstä

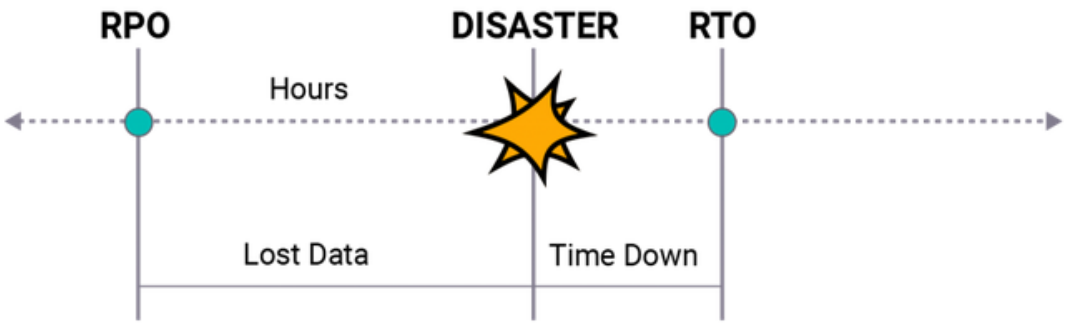
3.6.2 Palautumisaikatavoite

Palautumisaikatavoite (engl. Recovery Time Objective, RTO) kuvastaa aikaa, jossa määritellään, kuinka kauan tietyn sovelluksen palauttaminen voi kestää, ennen kuin siitä aiheutuu suurta haittaa yrityksen toiminnalle. Hyvin suuren prioriteetin sovelluksille RTO voi olla minuutteja, jos varmuuskopiointi ja palauttaminen on suunniteltu järkevästi. RTO määrittää organisaation yleisen tavoitteen ja määrittää, kauanko organisaatio pärjää ilman IT-infrastruktuuria ja/tai -palveluita. (RTO (Recovery Time Objective) Explained 2019.)

3.6.3 Palautuspistetavoite

Palautuspistetavoite (engl. Recovery Point Objective, RPO) kuvastaa datan määrää, joka voidaan menettää ilman, että siitä koituu suurta haittaa. RPO:n avulla myös määritetään kuinka usein tieto pitää varmistaa. RPO:n määrittäminen on erittäin tärkeää, sillä katastrofin sattuessa riskit datan katoamiselle säilyvät vaikka olisi käytössä reaaliaikainen varmuuskopiointi. Jos varmuuskopiointi suoritetaan joka yö kello

00:00 ja katastrofi sattuu tapahtumaan aamulla kello 08:00, menetetään kello 00:00 – 08:00 välillä tapahtuneet muutokset tietoihin (ks. Kuvio 6). (Denis 2019.)



Kuvio 6. RTO vs RPO (Mt.)

3.7 Suunnitelman testaus ja ylläpito

Palautumissuunnitelman testaus auttaa varmistamaan, että yritys pystyy palauttamaan tiedot sekä kriittiset sovellukset ja jatkamaan normaalia toimintaa katkoksen jälkeen. Monesti yritykset jättävät palautumissuunnittelun pelkästään paperille, mutta eivät testaa sen toimintaa. Jos testaamiseen ei investoida resursseja, syntyy uusi riski, jossa palautumissuunnitelma ei toteudu kuten odotettiin, kun sitä oikeasti tarvitaan. Kommunikointi sekä datan ja sovellusten palauttaminen ovat yleensä pääpisteinä palautumissuunnittelun testauksessa. Palautumissuunnitelmaa suositellaan testaamaan ympäri vuoden tietyin väliajoin (esim. 3 kk välein) sisällyttämällä tämä testaus sitä tarvitsevien työntekijöiden koulutukseen (IT-henkilöstö, DR-tiimi) sekä isompiin huoltoikkunoihin. (Rouse 2018c.)

Testaamisen tavoitteena on selvittää, kattaako suunnitelma organisaation määrittämät RPO- sekä RTO -vaatimukset. Testaamisella voidaan myös havaita muita puutekohtia, joita voidaan parantaa entistä varmemman suunnitelman luomiseksi. Palautumissuunnitelman testausta voidaan tehdä kolmella eri tapaa:

1) **Käymällä suunnitelma läpi,** jossa suunnitelman omistaja ja muut suunnittelun ja toteutuksen jäsenet käyvät suunnitelman läpi yksityiskohtaisesti keskustellen ja etsien epäkohtia.

2) **'Tabletop -testing' mallilla,** jossa kaikki osalliset käyvät suunnitelman läpi yksi vaihe kerrallaan. Tämän tarkoituksena on selvittää, tietävätkö kaikki varmasti, mitä tehdä ja ettei jää epäselvyyksiä omasta roolista katastrofin sattuessa.

3) **Simulaatiolla,** jossa luodaan tietty skenaario ja simuloidaan katastrofi, esimerkiksi sovelluksen tietokannan korruptoituminen. Tällä testillä nähdään hyvin, ovatko prosessit ja resurssit mukaan lukien varmuuskopiointijärjestelmät ja palautumiskyky suunnitelman määrittelemällä tasolla. Simulaatiossa voidaan testata, missä ajassa tietyt sovellukset saadaan takaisin toimintakuntoon palautuksen jälkeen, ja nähdään, onko suunnitelman toteutukseen määritetty tarpeeksi resursseja ja onko tiimi tarpeeksi koulutettu suunnitelman läpivientiä varten. (Mt.)

Kuvio 7 esitetty esimerkkiskenaarioita, joita varten voidaan etukäteen harjoitella.

Scenario	Description	Importance
Disgruntled employee sabotages a critical assembly line.	While such events may occur infrequently, they are always a possibility, especially where security may be lax, e.g., lack of security cameras in critical production areas.	Someone who regularly works in a production area may, over time, identify potential weaknesses in the equipment and technology.
Employee enters critical process data incorrectly and fails to double-check the entry, and the resulting mistake causes a massive system outage.	Accuracy and care are two important criteria in any process-controlled environment; a simple keystroke could shut down a major system.	Improper entry of system commands and other coding is a potential problem; it may be necessary to build additional security challenges and checkpoints to minimize potential coding errors.

Kuvio 7. Esimerkkiskenaarioita (Mt.)

Testauksen muita tärkeitä osa-alueita ovat ajoitus, milloin sovellusta tai järjestelmää on viimeksi testattu? Jos esimerkiksi tietokannan palautuksen testauksesta on vuosia, voi tietokanta olla kasvanut niin suureksi, ettei sitä saada enää palautettua aikaisemmin määritetyn RTO:n puitteissa. Infrastruktuurimuutokset, onko tullut käyttöön uusia levyjärjestelmiä tai palvelimia? Näillä voi olla suuri vaikutus suunnitelman toiminnan kannalta. (Mt.)

Testiä toteuttaessa voidaan käyttää apuna ainakin näitä kohtia:

- Luodaan tarkka testaussuunnitelma
- Määritellään tavoitteet
- Määritetään testaus tiimi, johon sisältyy tarvittava koulutettu henkilöstö
- Määritetään tarkka testauksen kohde (tietty sovellus, järjestelmä, verkko)
- Dokumentoidaan tarkasti testauksessa käytetyt skriptit ja testisuunnitelma
- Varmistetaan, että testiympäristö on valmis, saatavilla eikä aiheuta kuormaa tuotantojärjestelmille testin alkaessa.
- Määritetään tarkka aikataulu, milloin alkaa ja kauanko kestää
- Jos ilmenee ongelmia, pysäytetään testi ja käydään tilanne läpi
- Päivitetään palautumissuunnitelma ajan tasalle heti testin jälkeen (Mt.)

Palautumissuunnitelman testaus on paljon laajempi käsite kuin itse palautustestaus, jossa keskitytään testaamaan tiedon tai sovelluksen varmuuskopioista palauttamista.

Palautumissuunnitelman testauksen tavoitteina voisi olla esimerkiksi tietyn sovelluksen palautustestaus tai tiimin kouluttaminen oikeaan tilanteeseen simuloidun testin avulla. Suunnitelma määräytyy hyvin pitkälle alussa määriteltyjen tavoitteiden mukaisesti, joten ne kannattaa rajata ja miettiä alkuun kunnolla. Mitä tarkemmin testi saadaan osumaan tiettyihin tavoitteisiin, sitä tehokkaampi testistä tulee.

Testausta suorittavan tiimin tulee olla teknillisesti koulutettu vastaamaan testattavista prosesseista sekä järjestelmistä. Tiimissä tulisi olla ainakin yksi ylemmän johtoportaan henkilö seuraamassa toimintaa ja kirjaamassa ylös tärkeitä huomioita testin edetessä. Jokaiselle henkilölle määritellään suunnitelmassa varahenkilö, jotka ovat samalla tavalla koulutettuja sekä ajan tasalla järjestelmistä. Varahenkilöitä hyödynnetään, jos alkuperäinen testissä määritelty henkilö ei ole tavoitettavissa esim. vakavan sairauden vuoksi.

Aikataulua suunnitellessa pitää muistaa ottaa huomioon myös mahdollisten sovellustoimittajien aikataulut. Kaikkien osapuolien tulisi olla samanaikaisesti saatavilla ja suurten tiimien aikatauluttaminen voi olla haastavaa. Aikataulu on myös tärkeä katsoa niin, ettei testauksesta aiheudu haittaa tuotantojärjestelmille.

Kohde voidaan tapauskohtaisesti määritellä hyvinkin tarkasti. Kaikki testaukset ovat erilaisia, sillä suunnitelmat ovat erilaisia jokaisen organisaation kohdalla. Tarkalla määrittelyllä testauksesta saadaan tehokas, koska voidaan keskittyä syvällisemmin esimerkiksi tietyn osa-alueen testaamiseen ilman, että siihen kuluu liikaa aikaa.

3.8 Disaster Recovery as a Service (DRaaS)

DR palveluita on ollut tarjolla jo kauan, mutta DRaaSin todellinen määritelmä on vielä hieman hämärässä. DRaaS on yksinkertaisuudessaan palvelu, joka antaa asiakkaalle mahdollisuuden nostaa ympäristön takaisin ylös multi-tenant pilvipalvelusta, josta voidaan maksaa käytön mukaan. Palvelun määrittävät yrityksen vuokraama CPU, RAM, tallennustila ja verkkoresurssit jaetussa ympäristössä, johon voidaan replikoida data ja palauttaa tarvittaessa sen sijaan, että yritys ylläpitäisi itse omaa DR ympäristöä. (DRaaS: Your New Favorite Cloud Service, n.d. 5.)

DRaaS on enemmän pienten ja keskisuurten yritysten mahdollisuus, sillä suurissa ja monimutkaisissa ympäristöissä hinnat alkavat nousta korkealle. DRaaS tarjoaa yksinkertaisen lähestymistavan saavuttaa yrityksen tavoitteet, jossa tarjotaan aina saatavilla olevaa palvelua. (Mts. 5)

Palvelun tarjoamista hyödyistä voidaan nostaa esille ainakin seuraavat:

1. Nopea palautuminen – Ympäristö voidaan nostaa ylös suoraan pilvialustalle, joka antaa aikaa korjata ongelmat omilla palvelimilla.
2. Hinnan hallinta – Oman DR ympäristön ylläpitäminen voi olla kallista, ulkoistat hallinnan kolmannelle osapuolelle.
3. Joustavuus – Antaa mahdollisuuden aktivoida resurssit vasta kun niitä tarvitsee, voit maksaa vain käytön mukaan.
4. Yksinkertaisuus – Uudet teknologiamahdollisuudet tekevät toteuttamisesta helpon, replikointi ja varmuuskopiointi voidaan suorittaa suoraan pilvikapasiteettiin. (Mts. 6)

4 Active Directory ja palautustestaus

4.1 Yleistä

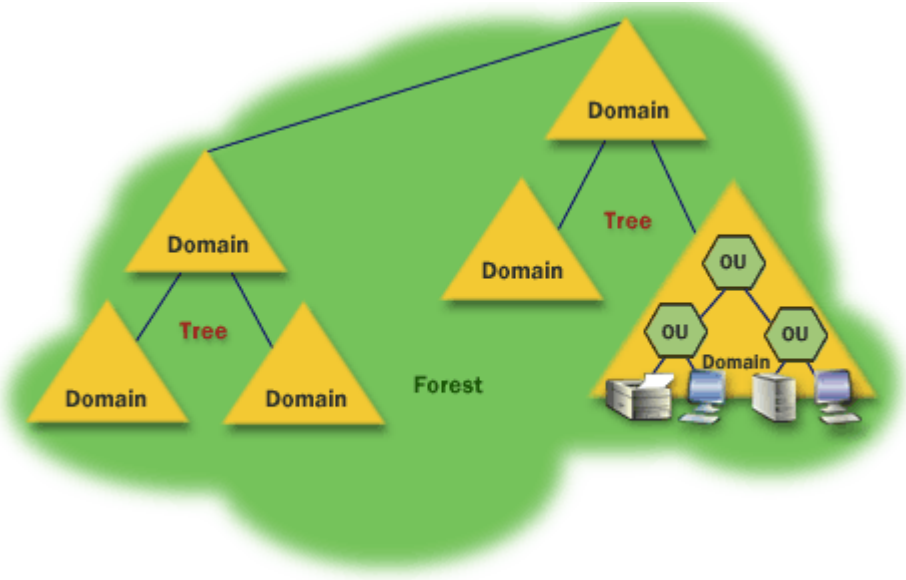
Työssä päätettiin toteuttaa esimerkkinä automaattisesta palautustestauksesta AD -palvelimen palautustestaus käyttämällä hyödyksi Veeamin Surebackup ominaisuutta, joka on suunniteltu testaamaan palautusta varmuuskopiosta sekä mahdollisia sovelluksia kuten Active Directoryä tai SQL -tietokantoja, joita palvelimelle on asennettu. Automaattisella palautustestauksella voidaan varmistaa, että AD -palvelimen hajoamisen sattuessa voidaan se myös palauttaa toimintakuntoon kivuttomasti ja nopeasti. AD:n palauttaminen on yleensä monimutkainen prosessi, jossa täytyy ottaa huomioon monia eri asioita kuten esimerkiksi metsän muut Domain Controllerit. Automatisoidulla palautustestauksella voidaan testata, että varmuuskopiointi on oikein konfiguroitu ja AD:n tietokannasta saadaan toimiva varmuuskopio.

4.2 Active Directory

4.2.1 Yleistä

Active Directory (AD) on Microsoftin kehittämä hakemistopalvelu, joka koostuu useista pienemmistä palveluista, joilla hallitaan oikeuksia ja pääsyä verkon resursseihin. Active Directory säilyttää datan objekteina, kuten käyttäjinä, ryhminä tai laitteina. Keskeisin AD -palveluista on Active Directory Domain Services (AD DS), joka tallentaa hakemistotietoja ja hallitsee käyttäjän kytkeytymistä toimialueeseen. AD DS varmistaa pääsyn, kun käyttäjä kirjautuu laitteeseen (palvelin, kannettava) verkon yli. Tällä voidaan myös hallita, kenellä on pääsy mihinkin verkon resursseihin esimerkiksi järjestelmänvalvojalla on yleensä laajempi pääsy ympäristöön kuin loppukäyttäjällä. (Rouse 2018a.)

AD:n rakenne koostuu pääasiassa metsästä (Forest), puista (Tree), toimialueista (Domain) sekä organisaatioyksiköistä (OU). Näiden yhteys toisiinsa on esitetty Kuvio 8.



Kuvio 8. Active Directoryn rakenne (Logical Structure and Areas of Active Directory n.d.)

Domain Controller

Domain Controller (DC) on palvelin, joka hallitsee AD:n käyttäjäryhmiä, käyttäjiä ja laitteita toimialueen sisällä pitäen huolen näiden autentikoinnista sekä oikeuksista. Kaikki käyttäjien tekemät pyynnöt lähetetään DC -palvelimelle, jossa ne tarkastetaan ja myönnetään tarvittavat oikeudet. DC -palvelimet ovat vielä todella yleisessä käytössä, mutta IT-infrastruktuurin siirtyessä enemmän julkipilven puolelle tarve hiipuu identiteetin ja pääsynhallinnan (IAM, Identity and Access Management) myötä. (Lujan 2019.)

4.2.2 Active Directoryn varmuuskopiointi

Yleensä Active Directory -palvelut suunnitellaan kahdennetusti. Tällä haetaan sitä, että DC -palvelimia on kaksi: toisen vikaantuessa voi näistä toinen ottaa ohjat ja jatkaa samoja tehtäviä, joita vikaantunut palvelin aikaisemmin hoiti. Tämä huomioon

ottaen Active Directory -palvelun saatavuus on yleensä korkea, mutta voi sattua myös tilanteita, milloin täytyy turvautua varmuuskopioista palauttamiseen.

Active Directory -palvelut organisoivat ja pitävät tietoa yksittäisistä objekteista metsän sisällä ja säilövät sen relaatiotietokantaan (ntds.dit -tiedosto). Aikaisemmin AD -palvelimen varmuuskopiointi oli monimutkaista: se sisälsi käyttöjärjestelmän sen hetkisen tilan varmuuskopioinnin erikseen. Veeam Backup & Replication hyödyntää 'Application Aware Image Processing' (AAIP) -teknologiaa suorittaakseen toimivan varmuuskopion virtuaalikoneesta ja sen palveluista. AAIP käyttää hyödyksi Microsoftin Volume Shadow Copy -palvelua, joka käskyttää käyttöjärjestelmän komponentteja valmistautumaan tilannekuvan (snapshot) ottamista varten. (Zhelezko 2016.)

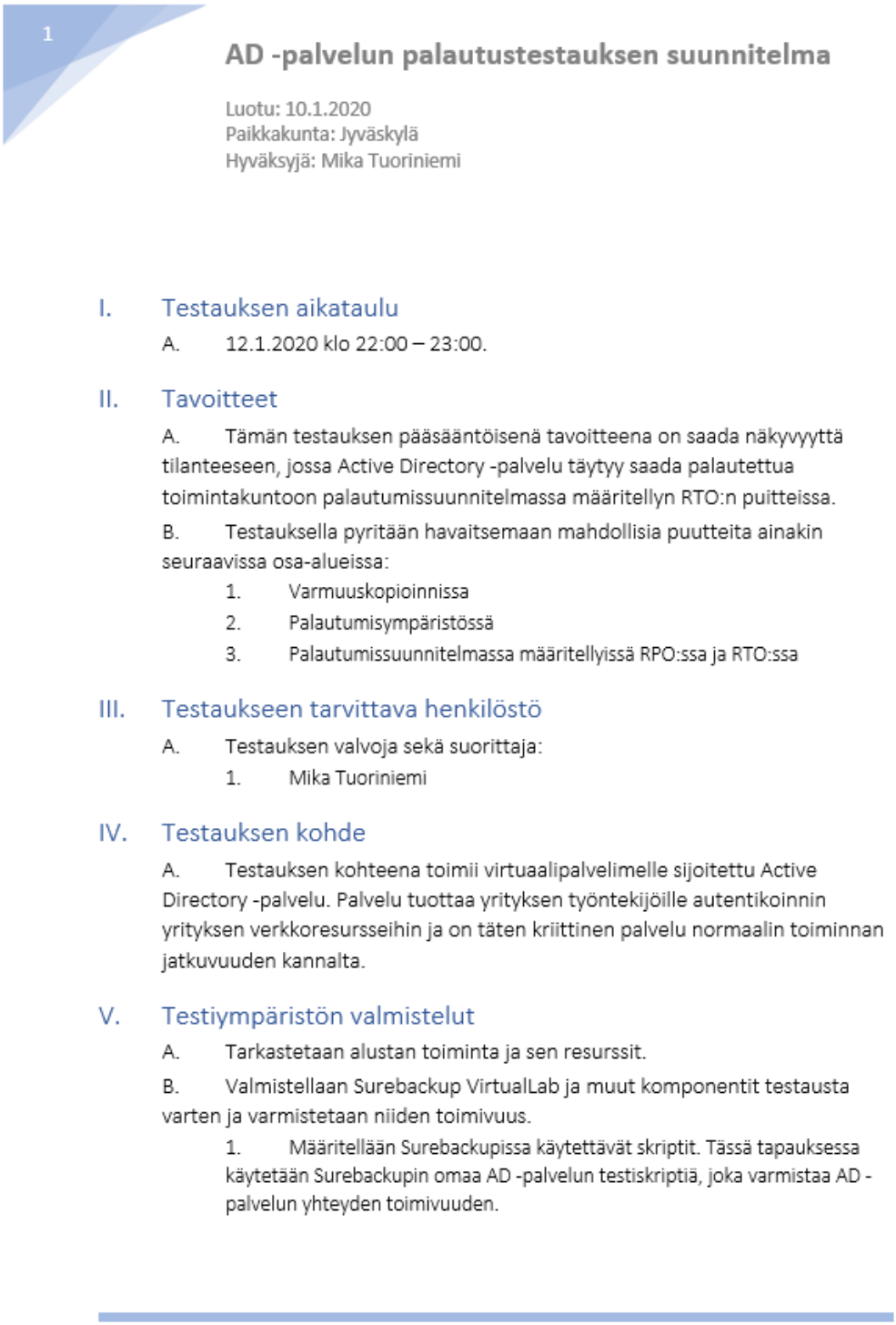
Jos Active Directory -palvelun varmuuskopiota suoritettaessa ei käytetä VSS -ominaisuutta, käyttöjärjestelmä ei viesti aktiiviselle tietokannalle tulevasta varmistuksesta, jolloin se voi jäädä epävakaaseen tilaan varmuuskopiota suorittaessa tehden siitä palauttamisen mahdottomaksi.

4.3 Palautustestaus

Mitä hyötyä varmuuskopioista on, jos varmuuskopioita ei voida todeta toimiviksi? Palautustestauksen (engl. Recovery Verification) tavoitteena on varmistaa, että varmuuskopioinnista palauttaminen onnistuu ja varmuuskopiot ovat onnistuneet oikein. Palautustestaus voidaan tehdä automatisoidusti tai manuaalisesti: manuaalisessa palautustestauksessa virtuaalinen palvelin palautetaan varmistuksesta virtualisointialustalle, minkä jälkeen se käynnistetään ja testataan sovellusten toiminta käsin. Automatisoidussa palautustestauksessa voidaan hyödyntää eri sovelluksia, kuten tässä työssä käytimme hyödyksi Veeamin Surebackup ominaisuutta. Automaattisessa palautustestauksessa käytetään hyödyksi eristettyä ympäristöä, johon haluttu virtuaalinen palvelin palautetaan, käynnistetään ja liitetään verkkoon automaattisesti, minkä jälkeen palvelinta vasten ajetaan erilaisia testejä toiminnan varmistamiseksi. Automatisoidun testin jälkeen palvelin voidaan jättää päälle, jos loppukäyttäjä haluaa itse kokeilla jonkin tietyn asian toimintaa.

Active Directory -palvelun palautustestauksessa on hyvä ottaa huomioon, ettei sitä palauteta alkuperäiseen sijaintiin, varsinkaan suoraan tuotantoverkkoon liitettynä. Tästä voi aiheutua konflikti alkuperäisen AD palvelimen ja palautetun välillä, mikä voi aiheuttaa katkoksia autentikointiin. Eristetyn ympäristön pystyttäminen tätä varten on hyvä varotoimi, ettei näin pääse käymään.

Palautustestausta varten olisi hyvä luoda erillinen suunnitelma, jossa esitellään testauksen kohde, aikataulu, tavoitteet sekä testauksen toteuttava henkilöstö. Suunnitelman tekeminen ei kuitenkaan ole pakollista, mutta se voi helpottaa testin suorittamista ja rajausta. Testaussuunnitelma voisi näyttää alla olevan kuvion mukaiselta (ks. Kuvio 9).



1

AD -palvelun palautustestauksen suunnitelma

Luotu: 10.1.2020
Paikkakunta: Jyväskylä
Hyväksyjä: Mika Tuoriniemi

I. Testauksen aikataulu

A. 12.1.2020 klo 22:00 – 23:00.

II. Tavoitteet

A. Tämän testauksen pääsääntöisenä tavoitteena on saada näkyvyyttä tilanteeseen, jossa Active Directory -palvelu täytyy saada palautettua toimintakuntoon palautumissuunnitelmassa määritellyn RTO:n puitteissa.

B. Testauksella pyritään havaitsemaan mahdollisia puutteita ainakin seuraavissa osa-alueissa:

1. Varmuuskopioinnissa
2. Palautumisympäristössä
3. Palautumissuunnitelmassa määritellyissä RPO:ssa ja RTO:ssa

III. Testaukseen tarvittava henkilöstö

A. Testauksen valvoja sekä suorittaja:

1. Mika Tuoriniemi

IV. Testauksen kohde

A. Testauksen kohteena toimii virtuaalipalvelimelle sijoitettu Active Directory -palvelu. Palvelu tuottaa yrityksen työntekijöille autentikoinnin yrityksen verkkoresursseihin ja on täten kriittinen palvelu normaalin toiminnan jatkuvuuden kannalta.

V. Testiympäristön valmistelut

A. Tarkastetaan alustan toiminta ja sen resurssit.

B. Valmistellaan Surebackup VirtualLab ja muut komponentit testausta varten ja varmistetaan niiden toimivuus.

1. Määritellään Surebackupissa käytettävät skriptit. Tässä tapauksessa käytetään Surebackupin omaa AD -palvelun testiskriptiä, joka varmistaa AD -palvelun yhteyden toimivuuden.

Kuvio 9. Testaussuunnitelma

Testaussuunnitelman luominen helpottaa myös mahdollisen testausraportin teke-
mistä. Testausraportissa olisi hyvä näkyä suunnitelman kohtien lisäksi testin tulokset

sekä mahdolliset ongelmakohdat, jotta niitä voidaan selvittää ja varmistaa, ettei kyseisiä ongelmia tule vastaan myöhemmin.

5 Veeam Surebackup

5.1 Yleistä

Surebackup on Veeam Backup & Replication tuoteperheen toiminnallisuus, joka antaa mahdollisuudet testata varmuuskopiosta palauttamista kokonaan eristetyssä ympäristössä. Tässä työssä kuvataan Surebackup toiminnallisuutta VMWare ESXi -alustalla. Teknologiaa voi hyödyntää myös Microsoftin Hyper-V virtualisointialustalla, mutta se eroaa hieman VMWaren toteutuksesta. SureBackupilla voidaan varmistaa palautuspisteiden toimivuus varmuuskopioidusta virtuaalikoneesta turvallisesti alkuperäisellä konfiguraatiolla ilman, että siitä on haittaa tuotantojärjestelmille.

Surebackup käyttää apuna normaalia imagepohjaista varmuuskopiota ja suorittaa seuraavat toimenpiteet testauksessa:

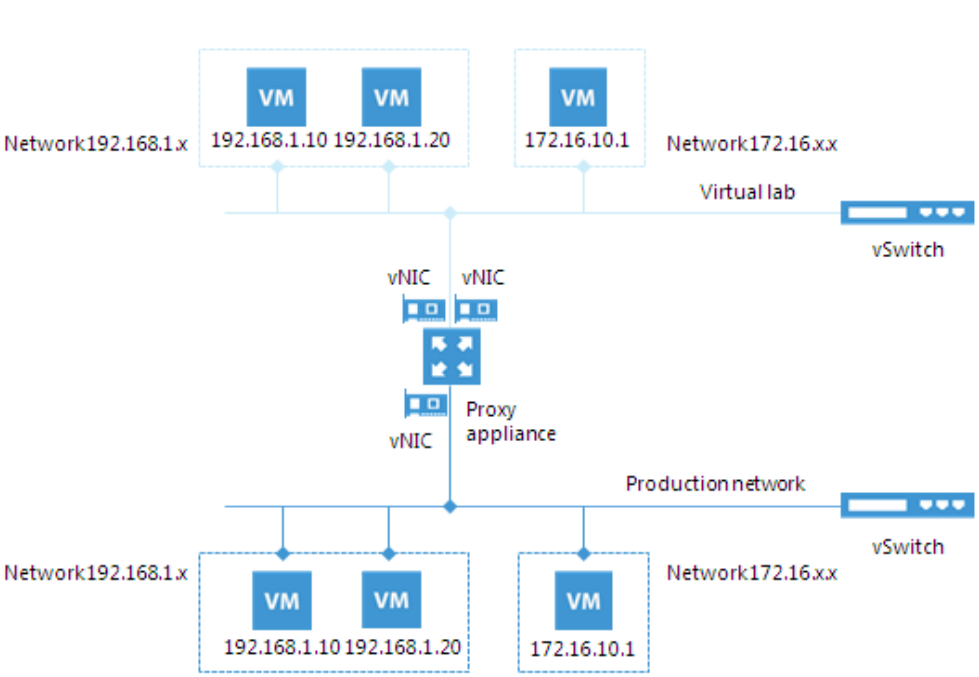
- Application Groupissa määritetyt virtuaalikoneet luodaan määritellylle alustalle ja liitetään eristettyyn VirtualLabiin. Virtuaalikoneet käynnistetään suoraan varmuuskopiosta hyödyntäen Veeam vPower NFS -palvelua, varmuuskopiota ei tarvitse ensin purkaa levylle.
- Jos Surebackup työ on määritetty ajamaan haittaohjelmaskannaus, se suoritetaan seuraavaksi.
- Virtuaalikoneille suoritetaan ennaltamäärätettyjä testejä: heartbeat testi, ping testi ja sovellustesti.
- Kun testaus on suoritettu, palautetut virtuaalikoneet sammutetaan, poistetaan ja testistä lähetetään halutessa raportti sähköpostilla. (How SureBackup works 2019.)

Surebackup vaatii kolme komponenttia toimiakseen:

1) Application Groupin, jossa määritetään testattava kone tai koneet. Tähän voidaan määritellä useita koneita, jotka ovat riippuvaisia toisistaan ja käynnistää ne halutussa järjestyksessä, jos vaaditaan jonkin toisen palvelimen olevan päällä ennen muita.
2) VirtualLabin, joka mahdollistaa eristetyn ympäristön, jossa palvelimet käynnistetään ja testataan.

3) Surebackup työn, minkä kautta testi suoritetaan. Tämä voidaan ajastaa automaattiseksi tai suorittaa manuaalisesti halutessa. (Mt.)

VirtualLab ei itsessään vaadi resursseja alustalta, mutta eristetyssä ympäristössä toimivat virtuaalikoneet käyttävät alustan resursseja kuten muutkin virtuaalikoneet. VirtualLabin verkoissa virtuaalikoneilla on samat IP-osoitteet kuin tuotantoverkon virtuaalikoneilla. Tämä mahdollistaa sen, että virtuaalikoneet voivat kommunikoida keskenään ilman konfiguraatiomuutoksia (ks. Kuvio 10). (Virtual Lab 2019.)



Kuvio 10. VirtualLab arkkitehtuuri (Mt.)

5.2 Testit

Testit, joita surebackup suorittaa ovat ennaltamääritettyjä. **Heartbeat** testi odottaa signaalia virtuaalikoneen VMWare Tools -komponentilta, jolla määritellään, onko käyttöjärjestelmä päällä. Jos signaali tulee tietyn väliajoin, testi menee läpi. **Ping** testi koittaa pingata virtuaalikonetta varmistuspalvelimelta. Jos virtuaalikone vastaa pingiin, testi menee läpi. Heartbeat ja ping testiä varten virtuaalikoneella pitää olla

VMWare Tools asennettuna. Jos tätä ei ole, testit jätetään väliin. **Application** testi odottaa sovellusten käynnistymistä ja suorittaa näitä varten määritellyn skriptin. Skriptejä on kahdenlaisia:

1) AD-, DNS-, catalog-, mail- sekä web -palvelimille käytetään skriptiä, joka yrittää saada yhteyttä johonkin tiettyyn sovelluksen porttiin. Esimerkiksi domain controlleria testatessa yritetään saada vastaus portin 389 kautta. Jos vastaus saadaan, testi menee läpi.
2) SQL palvelinta varten käytetään skriptiä, joka yrittää saada yhteyden tietokanta instansseihin ja itse tietokantoihin SQL palvelimella. (Backup Recovery Verification Tests 2019.)

Edellä mainittujen testien lisäksi voidaan suorittaa varmuuskopion validointi. Validointi suoritetaan CRC (Cyclic Redundancy Check) -tarkastuksella. Varmuuskopiota suoritettaessa lasketaan tarkistussumma jokaisesta blokista varmuuskopiossa ja säilötään tulos varmuuskopioon muun datan lisäksi. Validointia suoritettaessa varmuuskopio puretaan, lasketaan uusi tarkistussumma ja verrataan näitä kahta keskenään. Jos ne ovat samat, testi menee läpi. (Mt.)

6 Toteutus

6.1 Testiympäristö

Testiympäristönä käytettiin yksittäisen Dell PowerEdge R710 palvelimelle asennettua VMWare ESXi -virtualisointialustaa. Virtualisointialusta oli kirjoitushetkellä versiossa 6.7.0 Update 3 (Build 15160138). Alustalla (ESXi-01.lab.net) on kaksi kappaletta Intel Xeon L5640 prosessoria, 24Gb RAM ja 2x2TB HDD kiintolevyä. Molemmista kiintolevyistä luotiin omat datastoret.

Varmuuskopiointia varten käytettiin virtuaalipalvelinta. Windows Server 2019 käyttöjärjestelmällä varustetulle virtuaalipalvelimelle asennettiin Veeam Backup & Replication 9.5 Update 4b sovellus. Varmistuspalvelimella oli käytössään 6x vCPU, 8GB RAM

ja kaksi virtuaalista kiintolevyä eri datastoreilta. 100GB C-levy määritettiin käyttöjärjestelmää varten ja 500GB varmuuskopioita varten. Varmistuspalvelimelle asetettiin verkoiksi LAN sekä WAN (ks. Kuvio 11), jotka ovat eri VLANeissa (Virtual Local Area Network). Tässä tapauksessa LAN -verkko (10.10.10.0/24) on virtuaalikoneita varten luotu eristetty verkko, WAN -verkon (192.168.1.0/24) liikenne kulkee reitittimen kautta internettiin asti. WAN -verkko palvelimelle asetettiin sitä varten, että saatiin yhteys varmistettavaan alustaan ja voitiin asentaa tarvittavat sovellukset virtuaalipalvelimelle.

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : BACKUP
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter LAN:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-F8-38-8A
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.10.10.123(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter WAN:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection #2
   Physical Address. . . . . . . . . : 00-0C-29-F8-38-94
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.94(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Kuvio 11. BACKUP palvelimen verkkokonfiguraatio

Active Directory -palvelimena toimi myös Windows Server 2019 käyttöjärjestelmällä varustettu virtuaalipalvelin. Palvelimella oli 4x vCPU, 4GB RAM ja 100GB virtuaalinen kiintolevy käyttöjärjestelmää varten. Palvelimelle asennettiin Active Directory Do-

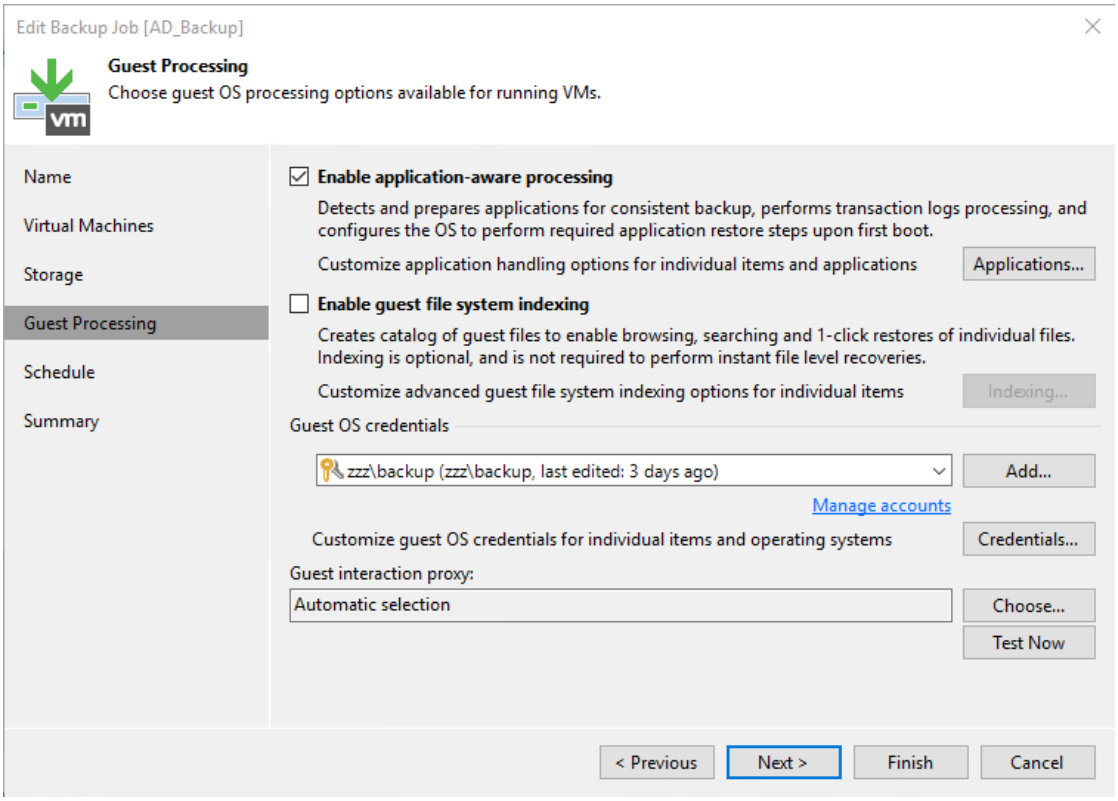
main Services -roolit Server Managerin kautta ja luotiin zzz.net toimialue. AD -palvelin liitettiin eristettyyn LAN -verkkoon 10.10.10.124 IP-osoitteella, josta sillä on yhteys BACKUP -palvelimeen (ks. Kuvio 12).

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : AD
   Primary Dns Suffix  . . . . . . . : zzz.net
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : zzz.net

Ethernet adapter LAN:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-3C-04-7C
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.10.10.124(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Kuvio 12. AD -palvelimen verkkokonfiguraatio

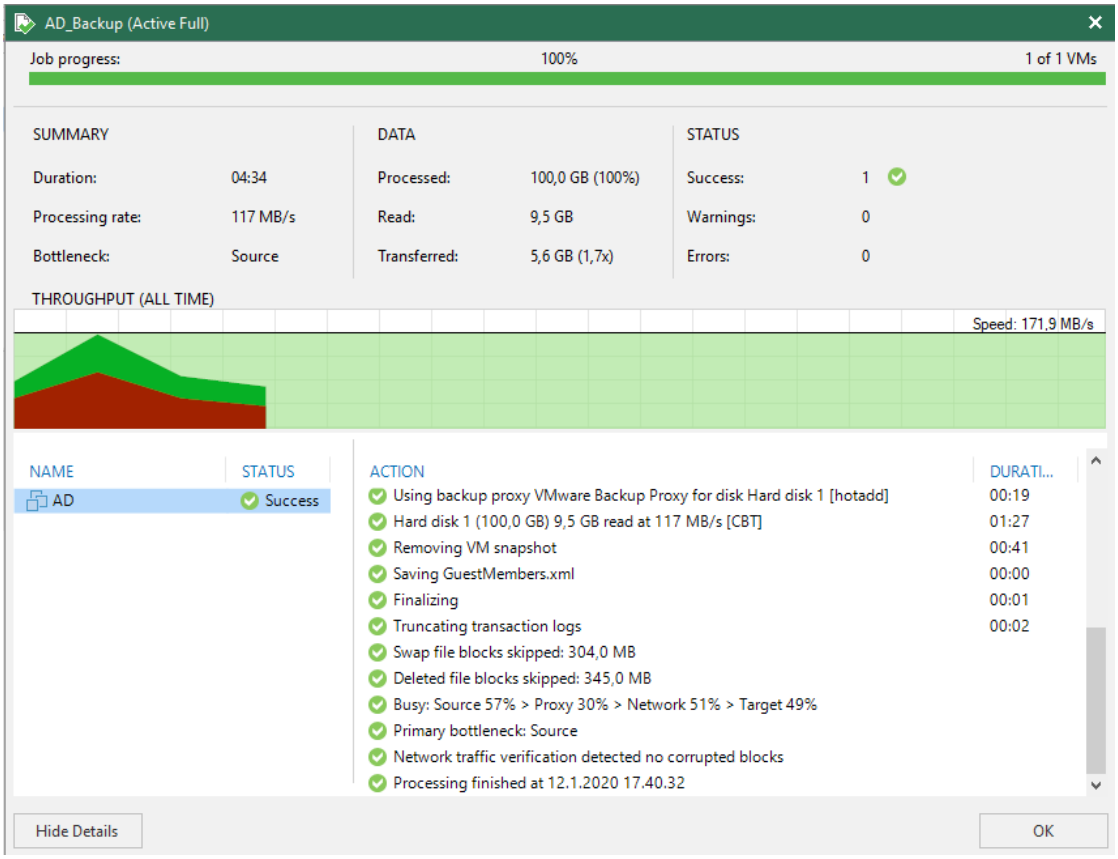
6.2 Varmuuskopiointi

Varmuuskopiointi AD -palvelimesta suoritettiin varmistuspalvelimen paikalliselle levylle. Varmuuskopiointia varten luotiin Domain Admin tasoinen käyttäjätunnus, joka asetettiin varmistustyöhön Guest Processingia (AAIP) varten (ks. Kuvio 13).



Kuvio 13. Guest Processing tunnus

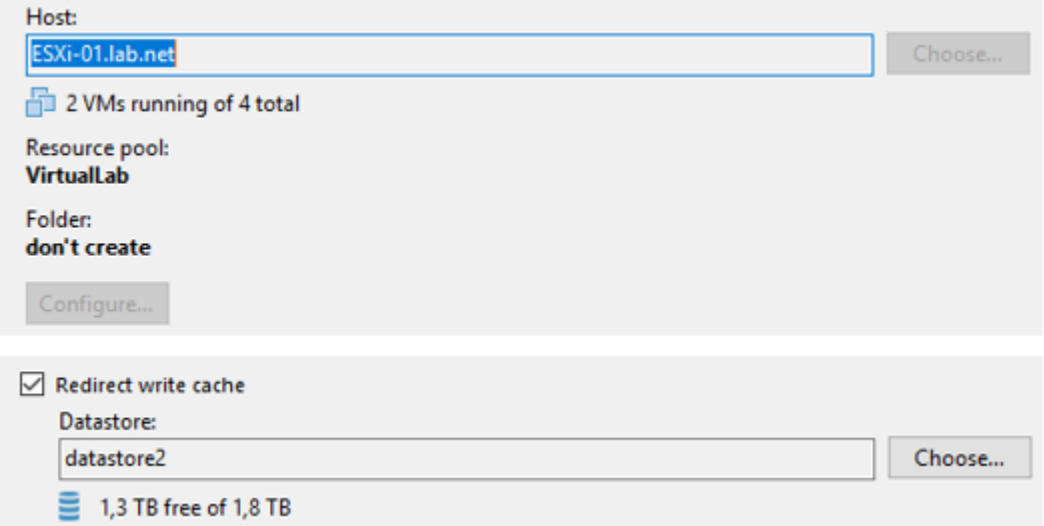
Alla olevassa kuviossa (ks. Kuvio 14) on esitetty onnistunut varmuuskopiointi ennen Surebackup testin ajoa. Testi voitaisiin myös määrittää suoritettavaksi suoraan varmuuskopioinnin jälkeen. Tällöin testiä ei täytyisi manuaalisesti ajaa yksittäisille palautuspisteille, vaan kaikki tulevat palautuspisteet voitaisiin testata automaattisesti niiden luonnin yhteydessä.



Kuvio 14. Onnistunut varmuuskopiointi AD -palvelimesta

6.3 Surebackup konfigurointi

Surebackup konfigurointi aloitettiin luomalla uusi VirtualLab. VirtualLab mahdollistaa eristetyn ympäristön virtualisointialustalla, johon testattavat virtuaalikoneet palautetaan suoraan varmistustiedostosta. VirtualLabille määritetään aluksi nimi ’VirtualLab’, minkä jälkeen valitaan palautusta varten käytettävä virtualisointialusta ja sen datastore Kuvio 15 mukaisesti.

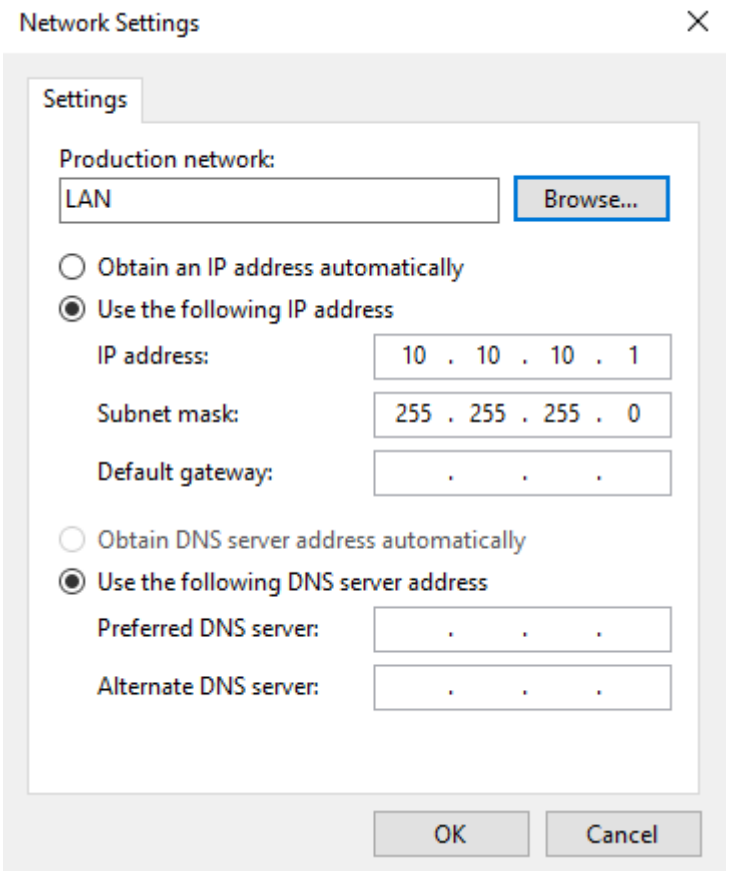


Kuvio 15. Valittu alusta sekä datastore

’Redirect write cache’ toiminnolla määritetään, minne palautetulla virtuaalikoneella tapahtuneiden muutosten sisältämät lokitiedostot säilötään. Uudelleenohjaamalla lokit toiselle datastorelle voidaan parantaa palautuksen suorituskykyä, mutta tämä tekee Storage vMotion toiminnosta mahdottoman ESXi 5.5 ja sitä aikaisemmilla versioilla. Heti testauksen jälkeen, lokitiedostot poistetaan. (Step 6. Select Destination for Virtual Disk Updates 2019.)

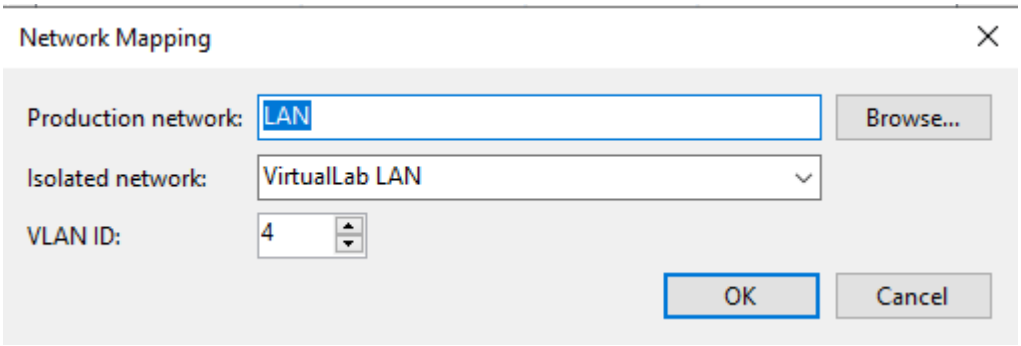
Konfiguroidaan käyttöön välityspalvelin, minkä kautta liikenne kulkee LAN -verkosta VirtualLabin eristettyyn VirtualLab LAN -verkkoon (ks. Kuvio 16). Välityspalvelimen tarkoitus on mahdollistaa kommunikointi tuotantoverkon sekä eristetyn verkon välillä. Välityspalvelin on Linux-pohjainen virtuaalikone, joka luodaan samalle alustalle VirtualLabin kanssa. Välityspalvelimelle määritellään IP -osoite tuotantoverkosta. (Proxy Appliance 2019.)

Välityspalvelin liitetään eristettyyn verkkoon sekä tuotantoverkkoon, joten sillä on näkyvyys molempiin. Välityspalvelin toimii käytännössä yhdyskäytävänä näiden kahden verkon välillä – se reitittää liikenteen tuotantoverkosta eristetyn verkon virtuaalikoneille. (Mt.)



Kuvio 16. Välityspalvelimen asetukset

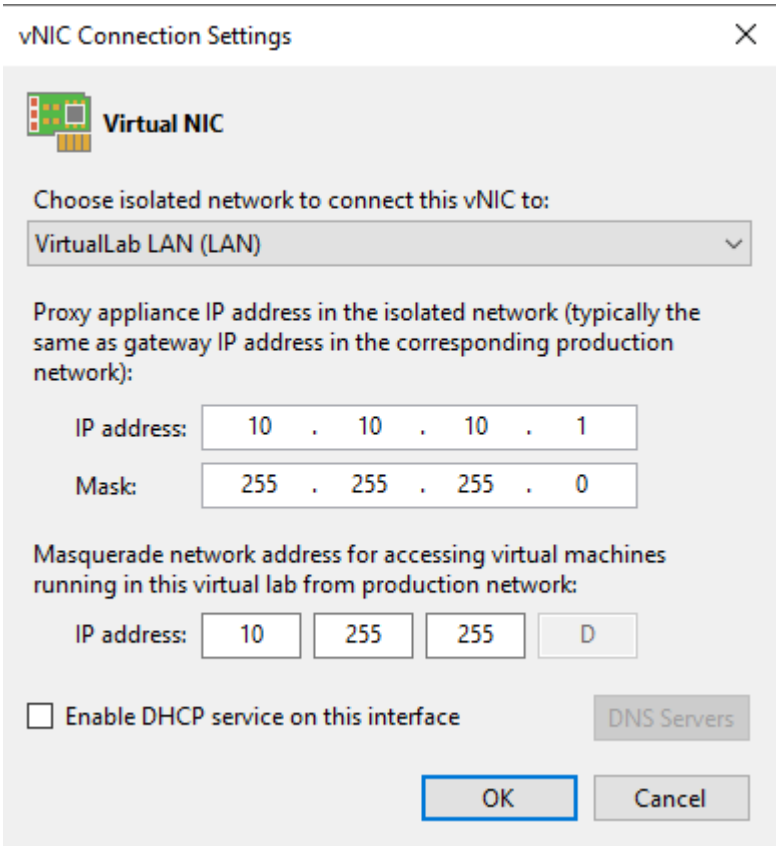
Välityspalvelimen määrityksen jälkeen valitaan tuotantoverkko ja luodaan sen perusteella eristetty verkko eri VLAN:iin, johon palautettu AD palvelin liitetään. Tässä tapauksessa loimme verkon nimeltä VirtualLab LAN ja asetimme sen VLAN:iin 4. (ks. Kuvio 17).



Kuvio 17. Verkkomappaus

Aikaisemmin määritellyn VirtualLab LAN -verkon perusteella määritettiin välityspalvelimen IP-osoitteeksi 10.10.10.1 ja luotiin masquerade IP-osoite avaruus (ks. Kuvio 18). Masquerade IP-osoite avaruus määrittää IP -osoitteet, joiden kautta mahdollistetaan pääsy palautetuille palvelimille toisesta verkosta. Hyöty tästä tulee siinä, että kun palautetulle koneelle kirjaudutaan, nähdään määriteltynä alkuperäinen 10.10.10.124 IP -osoite.

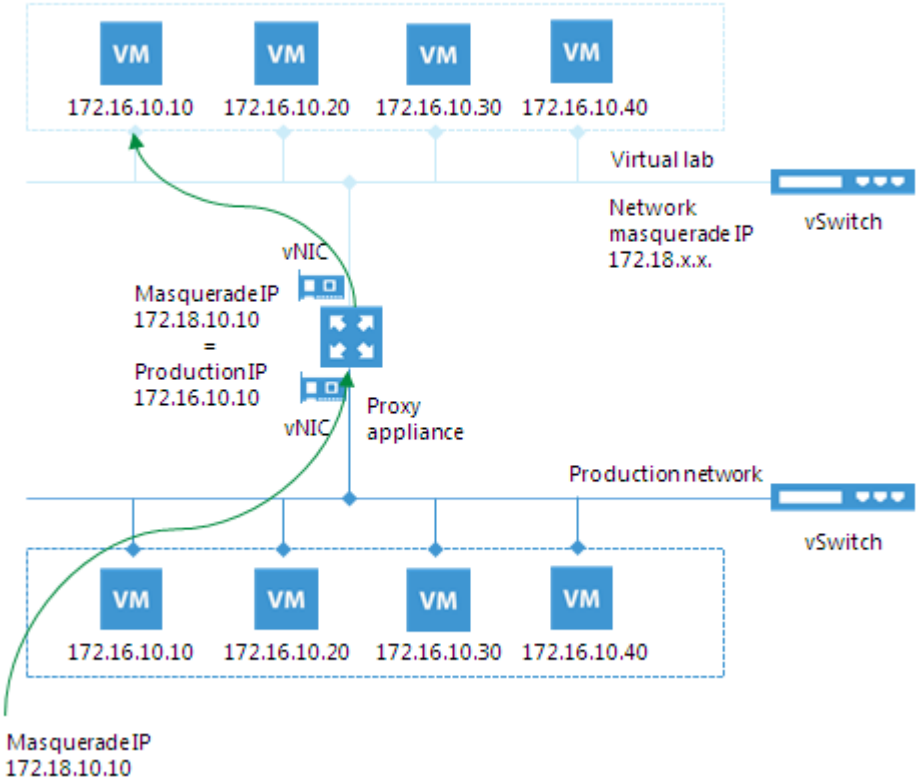
Jos tarkoitus olisi testata useita palvelimia samassa testissä, ne voisivat kommunikoida keskenään eristetyssä ympäristössä alkuperäisillä IP-osoitteilla kuten ne normaalisti tekisivät. Tämä on siitä syystä hyvä ominaisuus, ettei se vaadi erillisiä konfiguraatiomuutoksia testattaville palvelimille.



Kuvio 18. Masquerade IP-osoitteen määritys

Jokaisella VirtualLabin virtuaalikoneella on oma Masquerade IP-osoite tuotantoverkon IP-osoitteen lisäksi. Masquerade IP-osoite yleensä kuvastaa virtuaalikoneen IP-osoitetta tuotantoverkossa. Jos tuotantoverkossa sijaitsevan koneen IP-osoite olisi esimerkiksi 172.16.1.13, voisi Masquerade IP-osoite olla 172.18.1.13. (IP Masquerading 2019.)

Masquerade IP-osoite toimii sisääntulopisteenä eristetylle virtuaalikoneelle tuotantoverkosta. Kun halutaan kommunikoida tietyn virtuaalikoneen kanssa, käytetään sen masquerade IP-osoitetta. Alla olevassa kuviossa (ks. Kuvio 19) esitetty masquerade IP-osoitteen toiminnallisuus käytännössä. (Mt.)



Kuvio 19. Masquerade IP-osoite käytännössä (Mt.)

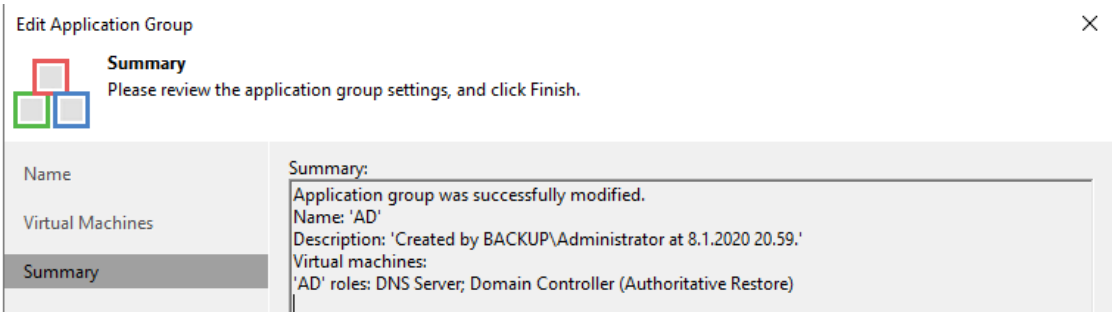
Monissa tapauksissa virtuaalikone ei toimi yksin vaan kommunikoi muiden palveluiden ja komponenttien kanssa. Tällaisen virtuaalikoneen testauksessa täytyy käynnistää ensin kaikki muut virtuaalikoneet, joista testattava palvelin on riippuvainen.

Nämä muut virtuaalikoneet voivat sisältää palveluita ja sovelluksia, joiden täytyy olla päällä ennen kuin testattava virtuaalikone voi toimia normaalisti. Tyypillisesti Application Group sisältää ainakin DC -palvelimen, DNS -palvelimen ja DHCP -palvelimen. (Application Group 2019.)

Application Grouppia määriteltäessä voidaan määrittää palvelimen rooli, käynnistys prioriteetti sekä viivästyttää käynnistystä, jotta aikaisempi virtuaalikone ehtii käynnistyä kokonaan ennen toisen virtuaalikoneen käynnistymistä. (Mt.)

Application Groupissa määriteltyjen virtuaalikoneiden tulee olla samalla alustalla, Hyper-V ja VMWare virtuaalikoneita ei voida laittaa samaan Application Grouppiin. (Mt.)

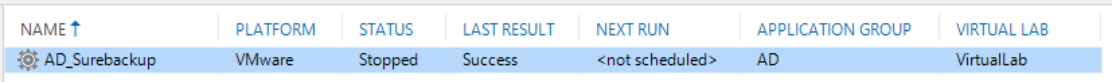
Alla olevassa kuviossa on esitetty testissä käytetyn Application Groupin asetukset (ks. Kuvio 20). Testiä varten luotiin Application Group, johon lisättiin testattava AD -palvelin ja sen rooleiksi asetettiin DNS, Domain Controller (Authoritative Restore).



Kuvio 20. Application Group

Näiden kahden komponentin luomisen jälkeen määritettiin Surebackup työ, minkä kautta itse testi suoritetaan (ks. Kuvio 21).

Surebackup työ kokoaa asetukset ja käytännöt palautustestauksen tehtävistä, kuten Application Groupin ja käytettävän VirtualLabin. Oletuksena voidaan käynnistää ja testata kolmea virtuaalikonetta samanaikaisesti. Tätä määrää voidaan myös nostaa, mutta jos testattavat virtuaalikoneet kuluttavat paljon resursseja, täytyy huomioida alustalla olevat vapaat resurssit. Mitä enemmän koneita testataan samanaikaisesti, sitä enemmän se vaikuttaa alustan suorituskykyyn ja testin pituuteen.

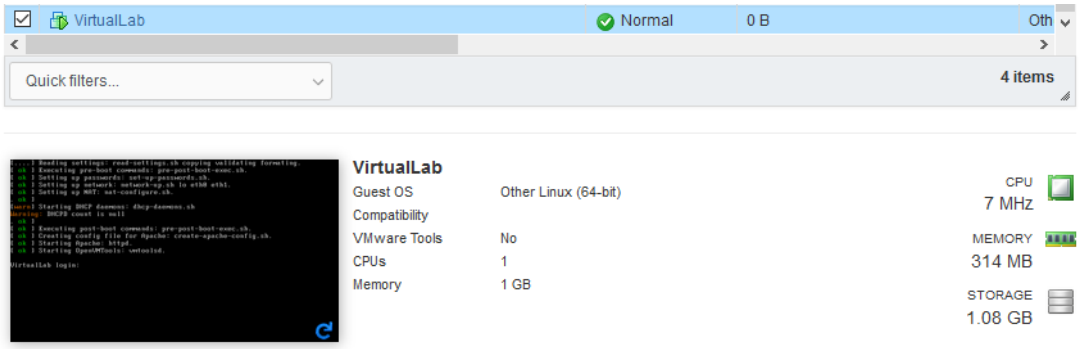


Kuvio 21. Surebackup työ

Oletuksena työn suorituksen jälkeen virtuaalikoneet sammutetaan, mutta tässä tapauksessa työ konfiguroitiin niin, että virtuaalikone jätetään päälle testin jälkeen. Näin voimme itse käydä tarkastamassa palautetun koneen toimivuuden ja suorittaa omia manuaalisia testejä halutessamme.

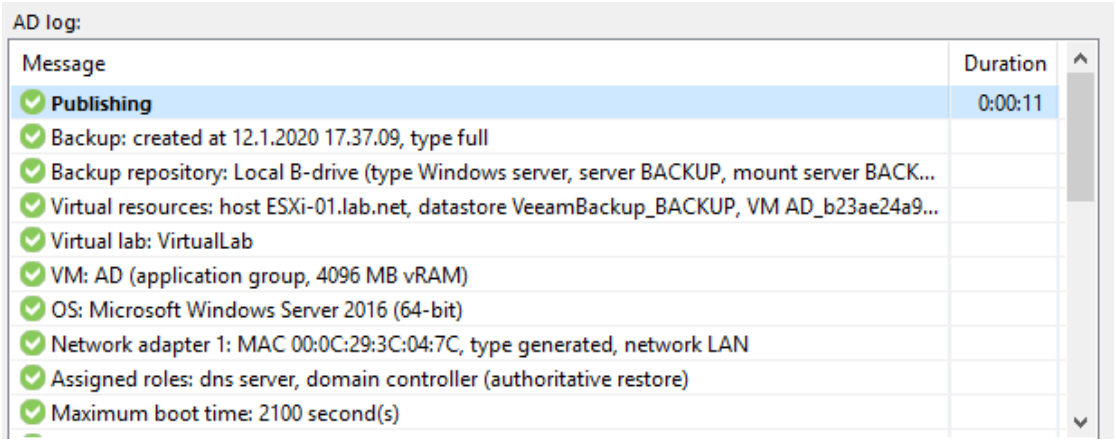
6.4 Testin suorittaminen

Testin käynnistyksen jälkeen Surebackup työ käynnistää VirtualLabin välityspalvelimen, joka näkyy alustalla yksittäisenä Linux -palvelimena. Välityspalvelimella on oletuksena 1x vCPU ja 1GB RAM (ks. Kuvio 22).



Kuvio 22. Välityspalvelin alustalla

Välityspalvelimen käynnistämisen jälkeen Application Groupin koneet julkaistaan alustalle. Surebackup käyttää palauttamisessa avuksi Veeamin *Instant VM Recovery* toimintoa, jossa virtuaalikoneet käynnistetään suoraan varmistustiedostosta. Tämä nopeuttaa palauttamista, sillä varmistustiedostoa ei tarvitse purkaa levylle palautusta varten (ks. Kuvio 23).



Kuvio 23. Virtuaalikoneen luonti

Julkaisun jälkeen virtuaalikoneen verkko liitettiin VirtualLabin sisäiseen verkkoon, jossa virtuaalikoneelle määritellään sama IP-osoite mikä sillä alkuperäisesti on (ks. Kuvio 24).

Verkot on luotu aikaisemmin VirtualLabin määrityksen jälkeen, tässä kohtaa testi ilmoittaa, että nämä ovat kunnossa ja niihin voitiin tehdä tarvittavat liitokset.

AD log:

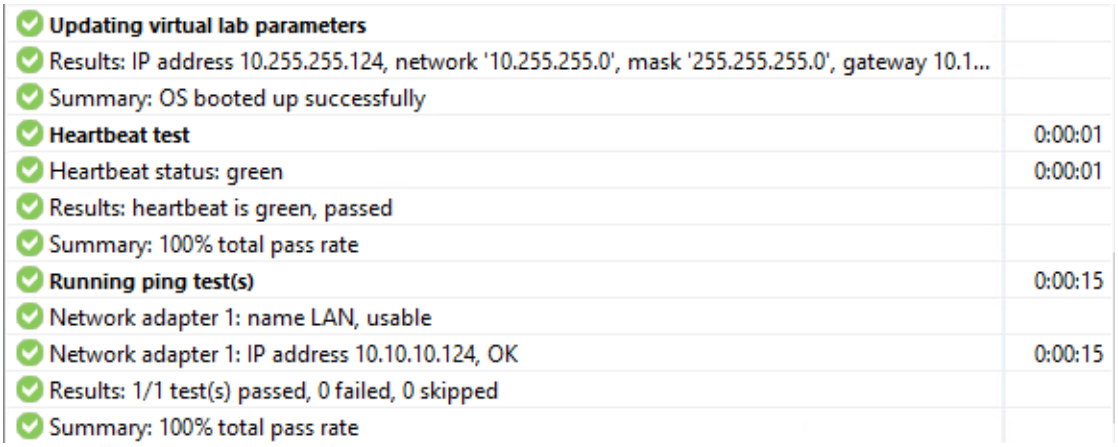
Message	Duration
Network 1: production LAN, isolated VirtualLab LAN, mapped	
Results: Networks: 1/1 mapped, 0 unmapped	
Summary: 100% test pass rate	
Registering	0:00:04
Configuring DC	0:00:24
Powering on	0:03:15
Waiting for OS to boot for up to 2100 seconds (stable IP algorithm)...	
Note: Will proceed to the next step at 12.1.2020 19.14.32 or earlier	
Results: IP address 10.10.10.124 is detected	

Kuvio 24. Verkon liittäminen

Virtuaalikone saa Masquerade IP-osoitteen verkkoavaruudesta, joka määriteltiin VirtualLabin konfigurointi osuudessa. Masquerade IP-osoite palautetulla virtuaalikoneella oli 10.255.255.124. Testi suoritti IP-osoitteen määrityksen jälkeen ensimmäiset heartbeat ja ping testit (ks. Kuvio 26). Heartbeat testi vaatii VMWare Toolsit varmuuskopioidulle virtuaalikoneelle. Surebackup työ lisää myös staattisen reitin varmistuspalvelimen reititystauluun, jossa määritellään reitti Masquerade verkkoon. Reitin yhdyskäytävänä toimii aiemmin määritetty välityspalvelin (ks. Kuvio 25)

```
C:\Users\Administrator>route print | find "10.255.255.0"
     10.255.255.0    255.255.255.0       10.10.10.1     10.10.10.123     26
```

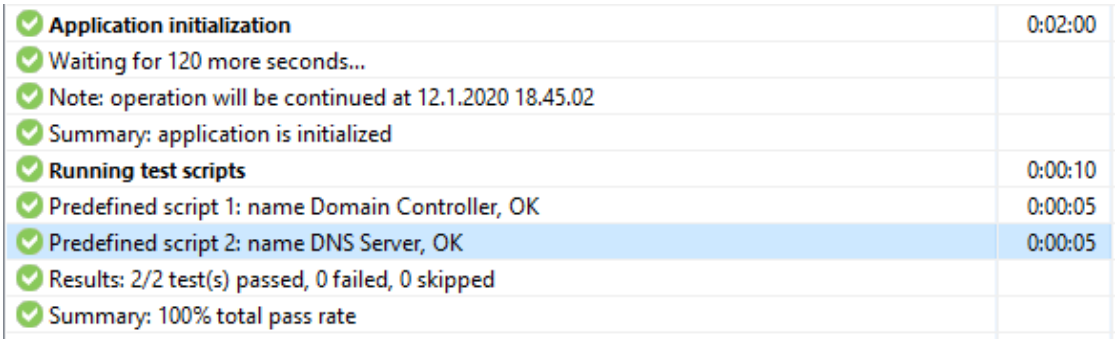
Kuvio 25. Reitti masquerade verkkoon testin aikana



Kuvio 26. Masquerade IP, heartbeat ja ping testi.

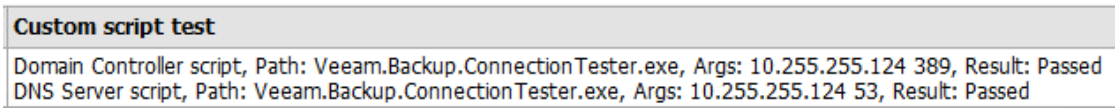
Tämän jälkeen työ suoritti määritellyn sovellustestin, johon aikaisemmin Application Grouppia luodessa määriteltiin Domain Controller (Authoritative Restore) ja DNS (ks. Kuvio 27).

Tässä testissä suoritettiin Authoritative Restore, joka palauttaa koko DC:n hakemiston siihen tilaan missä se oli, kun varmuuskopiointi suoritettiin. Hakemiston palautuksen jälkeen DC ilmoittaa palautetut tiedot muille metsän DC -palvelimille. Jos suoritettaisiin non-authoritative restore DC palautettaisiin myös samaan tilaan, mutta sen jälkeen palvelin vastaanottaisi kaikki tiedot mitä muilla DC -palvelimilla on. (Savill, J. 2003.)



Kuvio 27. Sovellustestit

Nämä testit kokeilevat saada yhteyttä tiettyihin sovelluksen portteihin todetakseen, että palvelu on päällä. Domain Controlleria testatessa otettiin yhteys porttiin 389 ja DNS -palvelua testatessa yhteys otettiin porttiin 53. Tässä nähtiin myös se, että varmistuspalvelin otti yhteyden Masquerade IP-osoitteeseen alkuperäisen sijasta (ks. Kuvio 28), vaikka virtuaalikoneelle oli määritelty 10.10.10.124 IP-osoite.



Kuvio 28. Domain Controller ja DNS komentosarjojen tulokset

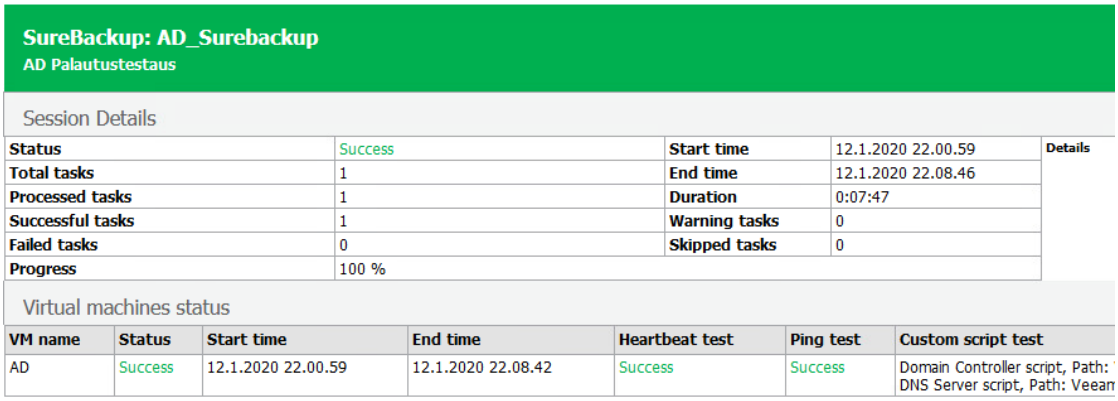
Automaattisten testien jälkeen palautettu virtuaalikone jätettiin päälle kuten haluttiin, jotta voitiin käydä tarkastamassa tilanne itse. Otimme etätyöpöytäyhteyden (RDP) palautetulle AD -palvelimelle, jossa suoritimme manuaalisen AD tietokannan tarkastuksen (ks. Kuvio 29).

```
C:\Windows\system32>net stop ntds
The following services are dependent on the Active Directory Domain Services service.
Stopping the Active Directory Domain Services service will also stop these services.

   Kerberos Key Distribution Center
   Intersite Messaging
   DNS Server
   DFS Replication

Do you want to continue this operation? (Y/N) [N]: y
The Kerberos Key Distribution Center service is stopping.
The Kerberos Key Distribution Center service was stopped successfully.


The Intersite Messaging service was stopped successfully.

The DNS Server service is stopping.
The DNS Server service was stopped successfully.

.
The DFS Replication service was stopped successfully.

The Active Directory Domain Services service is stopping.
The Active Directory Domain Services service was stopped successfully.


C:\Windows\system32>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: files
file maintenance: integrity
Doing Integrity Check for db: C:\Windows\NTDS\ntds.dit.

Checking database integrity.

                    Scanning  Status (omplete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................


Integrity check successful.
```

Kuvio 29. Manuaalinen ntds.dit kannan eheyden tarkastus

Tarkastuksen tarkoitus oli demonstroida sitä, että palautetulle palvelimelle voitiin itse kirjautua ja suorittaa haluttuja testejä myös manuaalisesti. Onnistuneen testauksen jälkeen Surebackup työ voidaan pysäyttää, jolloin virtuaalikone sekä välityspalvelin sammutetaan. Välityspalvelin jää alustalle virtuaalikoneeksi, mutta palautettu virtuaalikone poistetaan kokonaan.

Testistä on mahdollista saada raportti suoraan sähköpostiin, jossa näkyy testin lopullinen status, aloitus- ja lopetusaika, kesto, mitä virtuaalikoneita testattiin ja mitä komentosarjoja suoritettiin (ks. Kuvio 30).



SureBackup: AD_Surebackup
AD Palautustestaus

Session Details

Status	Success	**Start time**	12.1.2020 22.00.59	**Details**
Total tasks	1	**End time**	12.1.2020 22.08.46	
Processed tasks	1	**Duration**	0:07:47	
Successful tasks	1	**Warning tasks**	0	
Failed tasks	0	**Skipped tasks**	0	
Progress	100 %			

Virtual machines status

VM name	Status	Start time	End time	Heartbeat test	Ping test	Custom script test
AD	Success	12.1.2020 22.00.59	12.1.2020 22.08.42	Success	Success	Domain Controller script, Path: DNS Server script, Path: Veeam

Kuvio 30. Veeamin generoima raportti

Raportista nähdään, että tämän yksittäisen palvelun testaamisessa kesti noin 7 minuuttia. Tämä ei ole pitkä aika ottaen huomioon, että virtuaalikone luodaan tyhjästä, käynnistetään varmuuskopiosta, odotetaan palveluiden käynnistyminen ja suoritetaan testejä palveluita vasten. Testeistä voidaan luoda hyvinkin monimutkaisia, joilla saadaan automaattisesti testattua monia eri kokonaisuuksia esimerkiksi Web- ja SQL -palvelinten toimintaa keskenään. Raportti on hyvin pelkistetty, mutta se saadaan toimitettua suoraan testauksen jälkeen esimerkiksi testin luoneelle tiimille, jotka voivat varmistaa testin onnistuminen sen suorittamisen jälkeen ja korjata mahdolliset vikatilanteet.

7 Pohdinta ja johtopäätökset

Palautumissuunnittelu on laaja prosessi, joka vaatii monien eri sidosryhmien yhteystyötä ollakseen tehokas turva katastrofeja varten. Monessa tapauksessa palautumissuunnittelu voi olla kallis ja pitkä prosessi, mutta siitä saadut hyödyt voivat olla elintärkeitä yrityksen toiminnan jatkuvuuden kannalta. Nykypäivänä entistä useammat organisaatiot ovat ymmärtäneet palautumissuunnittelun tarpeellisuuden, sillä tiedon merkitys ja riskien määrä ovat kasvaneet vuosien saatossa.

Työn tarkoituksena oli tutkia palautumissuunnittelua yleisellä tasolla ja suorittaa automatisoitu palautustestaus virtualisoidulle Active Directory palvelulle. Pääsääntöisenä tavoitteena työllä oli saada yleinen ymmärrys palautumissuunnittelun osa-alueista, minkä pohjalta voidaan lähteä syventämään osaamista teorian ja käytännön tasolla.

Automatisoitu palautustestaus suoritettiin hyvin yksinkertaiselle, mutta erittäin yleiselle ja kriittiselle IT -järjestelmälle. Palautustestin tuloksista voidaan nähdä, että automatisoitu palautustestaus ei vaadi paljoa aikaa tai resursseja toteuttaa. Testi tuo esille kriittisiä asioita esimerkiksi RTO:n määrittelyyn, koska testauksella voidaan simuloida palveluiden palautumiseen kestävää aikaa. Testauksesta saadaan haluttaessa raportti, jossa näkyy mitä testejä suoritettiin ja kauanko testin läpiviennissä kestää. Tässä täytyy kuitenkin muistaa, että RTO vaihtelee kuormitustasojen mukana ja säännöllisellä testauksella voidaan varmistaa, että määritetty RTO pysyy tavoitettavissa datamäärien kasvaessa.

Työn tuloksena saatiin kattava katsaus palautumissuunnittelun sisältämistä osa-alueista, sekä tarkka toteutus AD -palvelun palautustestauksesta ja sen hyödyistä. Tutkimustuloksista on hyötyä niin työn tekijälle kuin myös toimeksiantajalle, työstä voidaan erotella palautumissuunnittelun eri vaiheet ja nähdä mitä niihin sisältyy, miksi palautumissuunnittelua tehdään ja miksi sitä tarvitaan. Palautustestauksesta saatiin luotua tarkka esimerkki, jota voidaan soveltaa melkein minkä tahansa palvelun automaattiseen palautustestaukseen.

Työ kasvatti omaa teknistä osaamista Surebackupin käytöstä ja kehitti näkemystä palautumissuunnittelusta isommassa mittakaavassa. Aikaisempaa näkemystä aiheeseen ei oikeastaan ollut yhtään, joten aluksi oli haastavaa lähteä rakentamaan järkevää rakennetta työlle. Rajausta ja tavoitetta tarkentaessa tämä kuitenkin helpottui, ja työssä päästiin mielestäni hyvään lopputulokseen.

Jatkokehityksen mielessä työhön voisi lisäksi koostaa malleja eri suuruisista varmistus- sekä palautumisympäristöistä. Näitä malleja voitaisiin käyttää hyödyksi esimerkiksi asiakkaiden varmistusympäristöjen suunnittelussa, kun tiedetään, millaista palautumiskykyä tavoitellaan.

Lähteet

Application Group. Surebackup dokumentaatio helpcenter.veeam.com verkkosivustolla. Viitattu 27.1.2020. https://helpcenter.veeam.com/docs/backup/vsphere/application_group.html?ver=95u4

Backup Recovery Verification Tests. 2019. Artikkeli helpcenter.veeam.com verkkosivustolla. Viitattu 10.1.2020. https://helpcenter.veeam.com/docs/backup/vsphere/surebackup_tests.html?ver=95u4

Bahan, C. 2003. The Disaster Recovery Plan. Artikkeli SANS instituutin reading roomissa, Viitattu 1.12.2019. https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164

Business Impact Analysis. N.d. Artikkeli ready.gov verkkosivustolla. Viitattu 16.12.2019. https://www.ready.gov/business-impact-analysis

Business Impact Analysis Worksheet. 2014. FEMA -järjestön tarjoama pohja BIA:n tekemistä varten. Viitattu 16.12.2019. https://www.fema.gov/media-library-data/1388776348838-b548b013b1cfc61fa92fc4332b615e05/Business_ImpactAnalysis_Worksheet_2014.pdf

Cook, G. N.d. What is a Disaster Recovery Team and Who Should be Included? Blogiposti flexential.com verkkosivustolla. Viitattu 9.1.2020. https://www.flexential.com/knowledge-center/blog/my-disaster-recovery-planning-team-who-should-be-included

Denis, G. 2019. RTO vs RPO: Two means toward the same end. Blogiposti cloudberrylab.com verkkosivustolla. Viitattu 18.12.2019.

Disaster Recovery. N.d. Artikkeli Georgetown Universityn verkkosivustolla. Viitattu 1.12.2019. https://continuity.georgetown.edu/dr

DRaaS: Your New Favorite Cloud Service. N.d. VeeamUP artikkeli Veeam.com verkkosivustolla. Viitattu 10.1.2020. https://www.veeam.com/veeamup-draas-cloud-service_wpp.pdf

How SureBackup works. 2019. Surebackup dokumenaatio helpcenter.veeam.com verkkosivustolla. Viitattu 10.1.2020. https://helpcenter.veeam.com/docs/backup/vsphere/surebackup_hiw.html?ver=95u4

IP Masquerading. 2019. Surebackup dokumentaatio helpcenter.veeam.com verkkosivustolla. Viitattu 27.1.2020. https://helpcenter.veeam.com/docs/backup/vsphere/surebackup_ip_masquerading.html?ver=95u4

Irwin, L. 2019. What is the ISO 27000 series of standards? Blogipostaus itgovernance.co.uk verkkosivustolla. Viitattu 4.12.2019. https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards

ISO 27000 Series of Standards. N.d. Artikkeli itgovernance.co.uk verkkosivustolla. Muokattu 08/2019. Viitattu 4.12.2019. https://www.itgovernance.co.uk/iso27000-family

Kenton, W. 2019. What is business continuity planning (BCP)? Artikkeli Investopedia.com verkkosivustolla. Viitattu 25.11.2019. https://www.investopedia.com/terms/b/business-continuity-planning.asp

Lavanya, N. & Malarvizhi, T. 2008. Risk analysis and management: a vital key to effective project management. Paper presented at PMI® Global Congress 2008—Asia Pacific, Sydney, New South Wales, Australia. Newtown Square, PA: Project Management Institute. https://www.pmi.org/learning/library/risk-analysis-project-management-7070

Liukko, S. & Perttula, S. 2019. Opinnäytetyön raportointi. Jyväskylä: Jyväskylän ammattikorkeakoulu. Viitattu 31.12.2019. http://oppimateriaalit.jamk.fi/raportointi/

Logical Structure and Areas of Active Directory. N.d. Artikkeli distributednetworks.com verkkosivustolla. Viitattu 31.12.2019. https://www.distributednetworks.com/active-directory-administration/module2/activeDirectory-logical-structure.php

Lujan, V. 2019. What Is A Domain Controller? Artikkeli jumpcloud.com verkkosivustolla. Viitattu 31.12.2019. https://jumpcloud.com/blog/what-is-a-domain-controller/

Mayer, A. 2017. The 3-2-1 Backup Rule – An Efficient Data Protection Strategy. Blogiposti Nakivo.com verkkosivustolla. Viitattu 18.12.2019. https://www.nakivo.com/blog/3-2-1-backup-rule-efficient-data-protection-strategy/

Proxy Appliance. 2019. Surebackup dokumentaatio helpcenter.veeam.com verkkosivustolla. Viitattu 27.1.2020. https://helpcenter.veeam.com/docs/backup/vsphere/surebackup_proxy_appliance.html?ver=95u4

Riskianalyysit. N.d. Artikkeli vtt.fi verkkosivustolla. Viitattu 9.1.2020. https://www.vtt.fi/palvelut/liiketoiminnan-kehitt%C3%A4minen/riskienhallinta/riskianalyysit

Riskienhallintaprosessi. N.d. Artikkeli Suomen Riskienhallintayhdistyksen verkkosivustolla. Viitattu 9.1.2020. https://www.pk-rh.fi/riskienhallintaprosessi.html

Rouse, M. 2018a. Active Directory. Artikkeli techtarget.com verkkosivustolla. Muokattu 06/2018. Viitattu 31.12.2019. https://searchwindowsserver.techtarget.com/definition/Active-Directory

Rouse, M. 2018b. Backup. Artikkeli techtarget.com verkkosivustolla. Muokattu 10/2018. Viitattu 18.12.2019. https://searchdatabackup.techtarget.com/definition/backup

Rouse, M. 2018c. Disaster Recovery (DR) test. Artikkeli techtarget.com verkkosivustolla. Muokattu 12/2018. Viitattu 18.12.2019. https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-DR-test

Rouse, M. 2018d. Risk Analysis. Artikkeli techtarget.com verkkosivustolla. Muotattu 06/2019. Viitattu 12.1.2020. https://searchsecurity.techtarget.com/definition/risk-analysis

RTO (Recovery Time Objective) Explained. 2019. Artikkeli IBM.com verkkosivustolla. Viitattu 18.12.2019. https://www.ibm.com/services/business-continuity/rto

Salleh, S. 2013. Business Impact Analysis for Disaster Recovery Planning And Beyond. Artikkeli lumina.com verkkosivustolla. Viitattu 16.12.2019. https://lumina.com/business-impact-analysis-for-disaster-recovery-planning-and-beyond/

Savill, J. 2003. What's the difference between an Active Directory (AD) authoritative and nonauthoritative restoration? Artikkeli itprotoday.com verkkosivustolla. Viitattu 12.1.2020. https://www.itprotoday.com/active-directory/whats-difference-between-active-directory-ad-authoritative-and-nonauthoritative

SFS-EN ISO/IEC 27000:2017. Tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 3.3.2017. Viitattu 4.12.2019. https://janet.finna.fi, SFS Online.

SFS-EN ISO/IEC 27001:2017. Tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 3.3.2017. Viitattu 4.12.2019. https://janet.finna.fi, SFS Online.

SFS-EN ISO/IEC 27002:2017. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 3.3.2017. Viitattu 4.12.2019. https://janet.finna.fi, SFS Online.

SFS-EN ISO/IEC 27005:2018. Tietoturvariskien hallinta. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 28.12.2018. Viitattu 4.12.2019. https://janet.finna.fi, SFS Online.

Step 6. Select Destination for Virtual Disk Updates. 2019. Instant VM Recovery dokumentaatio helpcenter.veeam.com verkkosivustolla. Viitattu 5.2.2020. https://helpcenter.veeam.com/docs/backup/vsphere/instant_recovery_datastore_vm.html?ver=95u4

Telia Inmics-Nebula. 2019. Artikkeli inmicsnebula.fi verkkosivustolla. Viitattu 16.1.2020. https://www.inmicsnebula.fi/fi/tietoa-yrityksesta

Tuominen, S. 2019. ISMS – Mikä se on ja mihin sitä tarvitaan? Blogipostaus mintsecurity.fi verkkosivustolla. Viitattu 4.12.2019. https://www.mintsecurity.fi/isms-mika-se-on-ja-mihin-sita-tarvitaan/

Veltsos, C. 2018. Lessons From the ISO/IEC 27005:2018 Security Risk Management Guidelines. Artikkeli SecurityIntelligence.com verkkosivustolla. Viitattu 18.12.2019. https://securityintelligence.com/lessons-from-the-iso-iec-270052018-security-risk-management-guidelines/

Virtual Lab. 2019. Surebackup dokumentaatio helpcenter.veeam.com verkkosivustolla. Viitattu 27.1.2020. https://helpcenter.veeam.com/docs/backup/vsphere/virtual_lab.html?ver=95u4

Walkowski, D. 2019. What is the CIA triad? Blogipostaus f5.com verkkosivustolla. Viitattu 10.1.2020. https://www.f5.com/labs/articles/education/what-is-the-cia-triad

Zhelezko, A. 2016. Backing up a Domain Controller: Best practices for AD protection (part 1). Blogiposti veeam.com verkkosivustolla. Viitattu 10.1.2020. https://www.veeam.com/blog/backing-up-domain-controller-best-practices-for-ad-protection.html